INFORMATION PRIVACY ::
A Spotlight on Key Issues

February 2004, Version 1.0

National Association of State
Chief Information Officers

About NASCIO

NASCIO represents the state chief information officers from the 50 states, six U.S. territories and the District of Columbia. Members include cabinet and senior level state officials responsible for information resource management. Other IT officials participate as associate members and private sector representatives may become corporate members.

Association Management Resources, Inc. (AMR) provides NASCIO's executive staff.

A MESSAGE FROM THE CHAIR

I am pleased to introduce a publication designed to educate policymakers at all levels of government on how private information should be protected in the Information Age.

Rapid advances in information technology have driven privacy to the forefront of the nation's public policy debate. NASCIO has taken a leadership role in this arena to influence national public policy and ensure that individual rights to privacy are protected. Consistent with our organization's Strategic Plan, *Information Privacy: A Spotlight on Key Issues* reflects NASCIO's commitment to the issue and our determination to educate, inform and guide states as they address this important new dynamic within the IT enterprise.

This comprehensive publication leverages the collective expertise of state CIOs to present a compelling and realistic starting point for states as they draft privacy policies that comply with federal and state law and protect information collected from the public. As public sector IT professionals and stewards of private information, it is critical that we take every reasonable and practical measure necessary to protect citizens' privacy and foster trust in government. This publication marks out the new frontier of the privacy issue and offers a roadmap to effective public policy.

I would like to thank the members of the NASCIO Privacy Committee and NASCIO staff who worked so diligently to produce this landmark publication. It is my hope that you will find it to be a vital asset.

Sincerely,

Stuart McKee
Chair, NASCIO Privacy Committee
Chief Information Officer
State of Washington

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

NASCIO would like to express its utmost gratitude to the Privacy Committee's Chair, Stuart McKee, CIO, Department of Information Services, State of Washington, and Vice Chair, Lester Nakamura, Administrator, Information and Communication Services Division, State of Hawaii, whose dedication to assisting the states in protecting citizen privacy made this publication possible. We very much appreciate their generosity with their time, energy and expertise. We also thank James T. Dillon, CIO, State of New York and Moira Gerety, CIO, State of New Mexico, for reviewing this publication on behalf of the NASCIO Executive Committee. NASCIO would also like to thank the following members of the Privacy Committee for lending their time and expertise to this publication:

Steven Adler, IBM Tivoli Security & Privacy
Scott Bream, State of Washington
Scott Cooper, HP
Richard Elwood, State of Idaho
William J. Ferguson, Carnegie Mellon University CIO Institute
Julie Spence Gefke, State of Colorado
Mike Gusky, State of Louisiana
John Halpin, 3Com
Jerry Johnson, State of Texas
Steve Kolodney, AMS
Roselyn Marcus, State of Washington
Mike McBrierty, SAS
Vanessa Mitra, State of Texas
Amy Moran, State of Wisconsin
Kym Patterson, State of Arkansas
Doug Robinson, Commonwealth of Kentucky
George Schu, VeriSign
Al Sherwood, State of Utah
Mark Smith, State of Ohio
David Sugarman, Network Associates, Inc.
Chris Tomlinson, State of Georgia
Jay Wack, Tecsec, Inc.
Hoyt M. Warren, Jr., CACI, Inc.
Colleen Woods, State of New Jersey
Donald Wray, State of Indiana
Gerard York, State of Florida

In addition, NASCIO would like to thank the following past members of the Privacy Committee for their contributions to this publication: P.K. Agarwal, ACS; Regenia David, formerly of the State of Minnesota; Martin Dunning, Sun Microsystems; Valerie McNevin, formerly of the State of Colorado; Carolyn Purcell, formerly of the State of Texas; Don Hildebrand, formerly of the State of Maine; Don McCorquodale, SAS; and Rick Shipley, State of Ohio.

NASCIO further thanks the states that contributed information on their privacy efforts to this publication.

Finally, NASCIO would like to thank Mary Gay Whitmer, NASCIO Issues Coordinator, for her work on this project, and Elizabeth VanMeter, NASCIO Executive Director; Matthew Trail, NASCIO Assistant Director; Robert Hansel, Project Associate; Chris Walls, AMR Senior Publications and Website Coordinator, and Barbara Denton, AMR Administrative Assistant, for their guidance, editorial revisions and other assistance regarding this publication.

Please direct any questions or comments about *Information Privacy: A Spotlight on Key Issues* to Mary Gay Whitmer at mwhitmer@amrinc.net or (859) 514-9209.

SECTION I: Executive Summary

Privacy has become an extremely important issue for both citizens and policymakers as personal information becomes more readily accessible via rapid advances in information technology. States possess a wide spectrum of citizens' personal information--from medical to financial to education information--placing CIOs in a unique position to provide insight and guidance on how to protect the privacy of citizens' information and, in so doing, building public confidence in government's ability to maintain the privacy of such information.

NASCIO has taken a leadership role—consistent with its Strategic Plan—and is willing to influence national public policy and ensure that individuals' rights to privacy are protected in the Information Age. NASCIO's ultimate goal is to ensure that states take reasonable and practical measures to protect citizens' privacy and foster citizens' trust in the government as a protector of their privacy rights.

Using this publication as an initial step, NASCIO is leveraging the collective expertise of state CIOs to educate policymakers within all levels of government on how private information should be protected in the Information Age.

This publication provides a starting point for states to help them develop privacy policies that protect citizen information and are compliant with federal and state legal requirements. Areas of information privacy that this publication addresses in Section III are:

- Children's Information
- Drivers' Information
- Health Information
- Financial Information
- Education Information
- Social Security Numbers
- Homeland Security-Related Information
- Website Privacy Policies
- Government Data Matching Activities and Agreements.

As background for those who are just learning about privacy-related issues, this publication provides:

- A discussion of the Federal Trade Commission's (FTC) Fair Information Use Principles that serve as the conceptual basis for many U.S. privacy policies (see Section III, Subsection A)
- A glossary of privacy-related definitions (see Appendix A)
- A detailed listing of major federal privacy developments (see Appendix B)
- A listing of privacy-related organizations (see Appendix C).

SECTION II: Introduction

Overview of Publication's Organization ::

NASCIO's *Information Privacy: A Spotlight on Key Issues* is intended to provide both a high-level overview of privacy-related issues as well as more detailed considerations for addressing privacy issues within the states. Below you will find a description of this publication's organization:

Section I is an Executive Summary that addresses NASCIO's organizational goals regarding the protection of citizen privacy and provides additional details about how the publication fits into NASCIO's overall strategic direction.

Section III provides detailed considerations for addressing specific information privacy issues.

- **Subsection A** discusses the fair information use principles that serve as a basis for the way that government and private sector entities address privacy issues in the U.S.
- **Subsection B** presents considerations for addressing privacy issues regarding:
  - ⇨ Children's Informatio
  - ⇨ Drivers' Informatio
  - ⇨ Health Informatio
  - ⇨ Financial Informatio
  - ⇨ Education Informatio
  - ⇨ Social Security Numbe
  - ⇨ Homeland Security-Related Informatio
- **Subsection C** provides detailed considerations for:
  - ⇨ Drafting website privacy policies
  - ⇨ Government data matching activities and agreements.

Appendix A contains a glossary of privacy-related definitions.

Appendix B outlines major privacy developments at the federal government level from 2000 through 2003 in such areas as children's, drivers', and health information. It also details recent privacy developments organized according to major federal players in privacy policy development, including the Department of Homeland Security and the Office of Management and Budget.

Appendix C describes selected privacy-related organizations.

Overview of Important Privacy Issues ::

The majority of this publication is dedicated to providing states with considerations to assist them in addressing the important privacy issues of the day. To this end, NASCIO has identified the following issues as being of importance to its members. Section III of this publication addresses in-depth each issue listed below:

Children's Information: An important issue for states and private sector entities is protecting the privacy of personal information that is collected from children online. Children's surfing of the Internet for both child-oriented websites and more general websites has raised the issue of what information should be collected from children by website operators, including state governments, and how website operators can use and/or disclose any children's personal information.

Drivers' Information: An issue of importance to the states is protecting the personally identifiable information that is contained in records maintained by state Departments of Motor Vehicles (state DMVs). State DMVs collect personal information from individuals when performing a variety of tasks, including issuing driver's licenses. This has raised the issue of when and to whom state DMVs can disclose personal information.

Health Information: An issue of importance for states and other entities is protecting individuals' personal health information. Both public and private entities, including hospitals, doctors' offices, and health care information clearinghouses, handle individuals' personal health-related information. This has raised questions about how an individual's health information may be used by such entities and when and how it can be disclosed to others. Another issue of importance is when and how an individual can access his or her own health information for review and correction, if necessary.

Financial Information: An issue of importance for both the public and private sectors is protecting the privacy of personal information that is collected by financial institutions, such as banks. Of particular concern regarding financial information is what type of personal information financial institutions can collect and when and to whom they can disclose that information. Another related concern is the commission of fraudulent acts in order to obtain personal information from financial institutions.

Students' Education Information: An issue of importance especially for educational institutions and agencies is protecting the privacy of personal information contained in students' education records. The collection of students' personal information has raised questions regarding when and to whom educational institutions and agencies may disclose students' personal information.

Social Security Numbers: An issue of importance is protecting the privacy of Social Security Numbers (SSNs). According to a May 2002 U.S. General Accounting Office report on SSNs, the SSN was created by the federal government in 1936 as an identifier of individuals for purposes of tracking workers' earnings and their eligibility for Social Security benefits. However, SSNs are currently used by state and local governments and the commercial sector. The use of SSNs as identifiers has raised concerns about the facilitation of identity theft through the unauthorized use of individuals' SSNs. Hence, those entities that collect, use or disclose individuals' SSNs must be careful to protect against their falling into the wrong hands.

Homeland Security-Related Information: An issue of importance to all levels of government is protecting the privacy of citizens' information while serving the interest of homeland security in preventing acts of domestic terrorism. With increased surveillance activities, information sharing, and a heightened emphasis on identifying individuals for various security-related purposes, the government also faces heightened concerns about the protection and use of citizens' personal information.

Drafting Website Privacy Policies: An issue of importance for all levels of government with an Internet presence is drafting website privacy policies to inform the public of what information may be collected from them and how that information may be used or disclosed.

Government Data Matching Activities and Agreements: An issue of importance is the ability of government agencies to match the information they possess on individuals with that of other government agencies. These types of matching activities allow the government to collect citizens' information less frequently and assist agencies in ensuring that they have more accurate citizen information. However, government data matching activities have raised concerns that the government will create "profiles" of individuals by compiling their personal information from multiple governmental agencies. Hence, government agencies must address such concerns when performing data matching activities.

SECTION III: Considerations for States on Information Privacy Issues

This section provides states and others with considerations for addressing information privacy issues for specific types of information, such as children's, health, and financial information (see Subsection B) and on drafting website privacy policies and conducting data matching activities (see Subsection C). In order to provide a theoretical basis for the considerations that are discussed in Subsections B and C, we first begin with a discussion of a few fundamental privacy principles.

SUBSECTION A: Fair Information Use Principles

In a 1998 report, the Federal Trade Commission (FTC) identified five "core principles of privacy protection" that were common to a series of studies in the U.S., Europe, and Canada regarding the collection, use, and privacy of personal information. These principles are:

- Notice/Awareness
- Choice/Consent
- Access/Participation
- Integrity/Security
- Enforcement/Redress.

The FTC characterized these principles as "widely-accepted." Below are a few basic points from the FTC's report about each of the five principles. You may consider these principles when drafting policies and procedures to protect the privacy of personal information.

- Link to the FTC's 1998 "Privacy Online: A Report to Congress": http://www.ftc.gov/reports/privacy3/toc.htm. *Note that this report also includes a section on fair information use principles as they apply to children's information.*

Notice/Awareness

- You should notify individuals of your information practices before you collect any personal information from them.
- You should provide individuals with notice of any rights they have to choose or consent to the collection or disclosure of information, of their rights to access and correct any personal information, how you protect the security and integrity of personal information, and how individuals may pursue any instances of non-compliance with your fair information practice policies and/or procedures.
- Other items of information that you may choose to include in a privacy notice are:
  - ⇨ *Identification of the entity collecting information*
  - ⇨ *How the information is collected (actively or passively)*
  - ⇨ *Nature of the information collected*
  - ⇨ *Whether an individual is required to divulge the information*
  - ⇨ *The consequences of an individual's refusal to provide the requested information*
  - ⇨ *How the collected information will be used*
  - ⇨ *Potential recipients of the information.*
- You should also make sure that your privacy notice is clear, placed in a prominent location, and is readily accessible from your website's homepage and any webpages where your website collects information from an individual.

Choice/Consent

- You should give individuals a choice about how their personal information may be used once collected.
- There are two basic regimes for providing a choice regarding the use of personal information:
  - ⇨ *Under an Opt-In Approach, an individual must take affirmative steps to allow you to collect and/or use his or her information.*
  - ⇨ *Under an Opt-Out Approach, an individual must take affirmative steps to prevent you from collecting and/or using his or her information.*
- You should provide individuals with a simple and easy way to exercise their choice regarding the collection and use of their personal information.

Access/Participation

- You should allow an individual the right to access and inspect his or her personal information.
- You should allow an individual the right to correct any inaccurate personal information.
- To ensure that an individual's access to his or her information is meaningful, the FTC provides the following measures as guidance:
  - ⇨ *Timely and inexpensive access to an individual's information*
  - ⇨ *A mechanism through which the collector of an individual's information can verify the information*
  - ⇨ *A simple means for an individual to contest the completeness and accuracy of his or her information*
  - ⇨ *A means for making corrections to an individual's information and notifying all recipients of the corrected information.*

Integrity/Security

- You should take reasonable steps to protect the integrity of information you collect, which may include:
  - ⇨ *Using only reputable sources of information*
  - ⇨ *Cross-referencing information against multiple sources*
  - ⇨ *Providing an individual access to his or her information*
  - ⇨ *Destroying out-of-date information or making it anonymous.*
- You should take both managerial and technical measures to ensure that information collected is protected against loss and unauthorized access, destruction, use or disclosure.
- Managerial security measures may include:
  - ⇨ *Within your organization, limiting those with access to information*
  - ⇨ *Ensuring those with access only use the information as authorized.*
- Technical security measures against unauthorized access may include:
  - ⇨ *Encrypting information that you transmit and store*
  - ⇨ *Limiting access to information through passwords*
  - ⇨ *Storing information on secure servers or computers that are not accessible by a modem.*

Enforcement/Redress

- The FTC stated in its report that the above-described core privacy protection principles "can only be effective if there is a mechanism in place to enforce them. Absent an enforcement

and redress mechanism, a fair information practice code is merely suggestive rather than prescriptive, and does not ensure compliance with core fair information practice principles."

- Among the options for enforcement, the FTC identified the following:
  - ***Self-regulation*** *through which an industry provides a mechanism to ensure that its members comply with a code of fair information practices and provides a means of redress for those individuals injured by a member of the industry who has failed to comply with the code of fair information practices.*
  - ***Private remedies for individuals*** *harmed by an entity's failure to comply with a code of fair information practices. Legislation is needed to implement this enforcement option.*
  - ***Government enforcement*** *of compliance with a fair information practices code through civil and/or criminal penalties*.

A Note on International Privacy Protections:

An earlier incarnation of the fair information use principles discussed above was developed by a task force of the U.S. Department of Health, Education and Welfare in 1973. That early version of the fair information use principles dealt with the collection, disclosure, secondary use, correction and securing of personal information. Over the years, these fair information use principles have evolved through the work of international entities, such as the Organisation for Economic Co-operation and Development (OECD), the Council of Europe, and the European Union.

When establishing privacy policies, it is important to note that the United States' approach to privacy differs somewhat from other countries' approaches. For example, while some countries have enacted omnibus data protection laws that embody versions of the fair information principles, the U.S. has not codified those principles in such a sweeping federal law. Instead, the fair information use principles form the basis of many U.S. laws that deal with the privacy of certain types of information, such as financial information and personal information held by the federal government. Another difference is the fact that other countries, such as Canada, Australia and New Zealand, have a privacy commissioner or similar position. The U.S. does not currently have a comparable position within the federal government, although such federal agencies as the Department of Homeland Security have a Chief Privacy Officer.

NASCIO would like to point out that other countries' privacy requirements could potentially become an issue when an individual from another country accesses a U.S. or state government website. In such situations, we recommend that you consult your general counsel regarding whether international law would dictate your adherence to any other countries' privacy requirements.

- Link to information about the OECD's information privacy efforts: http://www.oecd.org/document/26/0,2340,en_2649_34255_1814170_1_1_1_1,00.html.
- Link to information about the Council of Europe's information privacy efforts: http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Data_protection/.
- Link to information about the European Union's information privacy efforts: http://europa.eu.int/scadplus/leg/en/lvb/l14012.htm.

SUBSECTION B: Considerations for Addressing Privacy for Specific Types of Information

Children's Information ::

Important Information Privacy Issue

An important issue for states and private sector entities is protecting the privacy of personal information that is collected from children online. Children's surfing of the Internet for both child-oriented websites and more general websites has raised the issue of what information should be collected from children by website operators, including state governments, and how website operators can use and/or disclose any children's personal information.

Federal Authority on the Issue

The Children's Online Privacy Protection Act of 1998 (COPPA), 15 USC §§6501-6506.

- **What Does It Do?** COPPA's intent is to give parents a way to control the information that is collected from their children online. It places requirements on how children's personal information is collected online and can then be used and/or disclosed. COPPA generally requires commercial website operators of websites directed to children under 13 to provide notice of and obtain verifiable parental consent for the online collection, use and disclosure of children's personal information. Website operators cannot collect more personal information from a child than is reasonably necessary to participate in an online activity and must establish reasonable procedures to protect the security, integrity and confidentiality of children's information.

  When Congress enacted COPPA it provided the FTC (Federal Trade Commission) with authority to promulgate regulations that clarify and implement COPPA's requirements. COPPA's Final Rule provides additional detail about many aspects of COPPA including its notice and parental consent requirements.

- **To Whom Does It Apply?** COPPA applies to commercial website operators and online services that either are directed to children under 13 or that have actual knowledge of collecting personal information from children under 13. While COPPA does not appear to apply directly to the states, they can use its requirements as a guide for their own online collection of children's information.

  Note, though, that in its "Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002," the U.S. Office of Management and Budget (OMB) directed federal agencies to incorporate COPPA's requirements if they provide website content to children under 13 and collect personally identifiable information from such website visitors. OMB's privacy guidance also provides an attachment that includes a FTC summary of its guidance for federal agencies' compliance with COPPA. OMB's guidance regarding COPPA modifies a previous memorandum that it had issued directing all federal agencies and contractors to comply with COPPA's requirements for federal websites directed to children.

- **What Elements of Control Do States Have Regarding Children's Information?** As stated above, COPPA does not appear to directly apply to state government, thus providing states with flexibility in the way that they protect children's information that is collected online.

  States also have a role to play in the enforcement of COPPA as it applies to commercial website operators. While the FTC generally enforces COPPA, a state's Attorney General has the right to bring civil actions against commercial website operators that violate COPPA where there is a reason to believe that an interest of the state has been or is currently being threatened or adversely affected. However, COPPA prohibits state and local governments from imposing liability on website operators engaging in interstate or foreign commerce in a way that is inconsistent with COPPA and its Final Rule.

Link to COPPA [15 USC §§6501-6506]: http://www4.law.cornell.edu/uscode/15/ch91.html.

Link to the COPPA Final Rule [CFR Part 312]: http://www.ftc.gov/os/1999/10/64fr59888.pdf.

Link to OMB's 2003 Guidance for Federal Agencies [OMB Memorandum M-03-22]:
http://www.whitehouse.gov/omb/memoranda/m03-22.html.

Link to OMB's 2000 Guidance for Federal Agencies [OMB Memorandum M-00-13]:
http://www.whitehouse.gov/omb/memoranda/m00-13.html.

Application of this Privacy Issue

What Types of Children's Information are Involved in this Issue? If you collect the following types of personally identifying information from children, you may want to address how the information is collected and used and whether it will be disclosed to anyone else:

- A first and last name
- Home or physical address
- Email address
- Phone number
- Social Security Number
- Another identifier that the FTC determines could permit the physical or online contacting of a child
- Other information about a child or a child's parent that is combined with any of the above-described identifiers.

What Types of Activities are Involved in this Issue? If you perform the following types of activities, you may want to address privacy issues surrounding the collection of children's information online:

- If you collect personal information generally online (because there exists the possibility that a child could submit his or her information to you)
- If your website is directed to children under the age of 13 and you collect personal information from them directly or indirectly
- If you know that you are collecting information from children under the age of 13 regardless of whether your website is directed to children under 13.

Note that information can be collected directly from children or can be collected indirectly via a tracking mechanism such as a cookie.

Considerations for Addressing the Privacy of Children's Personal Information Collected Online

While COPPA does not appear to apply directly to state government, the following considerations have been derived from COPPA's provisions in order to provide states with a starting point for identifying potential privacy issues surrounding the collection of children's information online. The considerations in this section are potential ways in which a state might protect the privacy of children's information collected via state websites. You also may consider consulting OMB's guidance for federal agencies in complying with COPPA. A link to it is provided below.

- Link to OMB's "Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002" M-03-22: http://www.whitehouse.gov/omb/memoranda/m03-22.html.

Collecting Children's Information:

Consider the current status of your website regarding the collection of children's personal information online and evaluate:

- *Whether your website is directed to children, particularly those under 13 years of age*
- *Whether those operating your website have actual knowledge that they are collecting information from children directly or indirectly (such as through a cookie or other tracking mechanism)*
- *Whether any information that you collect from your website might be submitted by a child directly or indirectly.*

If your evaluation results in an affirmative answer under any of the above-listed scenarios, you may want to consider establishing policies on the collection of children's information.

If you do collect children's personal information online under any of the above-mentioned scenarios, collect no more personal information from children online than is reasonably necessary in order for the child to participate in an online activity, such as a game.

Providing Parents with Rights Regarding a Child's Information:

Obtain a parent's verifiable consent before collecting, using and/or disclosing his or her child's personal information.

Allow parents to agree to the collection of his or her child's personal information without agreeing to the disclosure of such information.

Provide a reasonable means for a parent to review the personal information that has been collected from his or her child. At a parent's request, you may inform him or her of the specific types and categories of personal information that have been collected from the child, such as:

- *Name*
- *Address*
- *Phone number*
- *Email address*
- *Hobbies*
- *Extracurricular activities.*

Ensure that the means you use to allow a parent to review his or her child's previously collected information is not unduly burdensome.

Ensure that the person requesting to review a child's information is the child's parent, taking into consideration the technology that is available for such verification.

- *OMB's 2003 privacy guidance states that federal agencies must use "reasonable procedures" to ensure that they are dealing with a child's parent. These procedures may include "obtaining a signed hard copy of identification, accepting and verifying a credit card number, taking calls from parents on a toll-free line staffed by trained personnel, email accompanied by a digital signature, or email accompanied by a PIN or password obtained through one of the verification methods above."*

Provide a reasonable means for a parent to:

- *Refuse the further collection of his or her child's personal information*
- *Refuse the further use of information previously collected from his or her child*
- *Direct the website operator to delete his or her child's previously collected information.*

Providing a Privacy Notice:

Post a notice on your website specifying your practices regarding the collection, use and disclosure of personal information.

- *OMB's 2003 privacy guidance requires the posting of a notice for federal agencies whose websites offer a separate area for children and collect personal information from them.*

Make sure the language of the notice is clear and understandable.

Make sure that the notice is complete in the information it contains. You may want to include one or more of the following elements of information in the notice:

- *Name, address, phone number, and email address of the website operator*
- *The types of personal information that are collected from children*
- *Whether children's personal information is collected directly or indirectly*
- *How children's personal information is or might be used*
- *Whether children's personal information is disclosed to third parties*
- *If children's personal information is disclosed to third parties, the types of business in which the third party is engaged, the general purposes for which such information is used, whether the third parties have agreed to maintain the confidentiality, security and integrity of children's personal information, and that a parent can consent to the collection and use of his or her child's information without consenting to its disclosure to third parties*
- *Statement that the operator cannot condition a child's participation in an activity upon the disclosure of more personal information than is reasonably necessary to participate in the activity*
- *Explain a parent's rights to review and delete his or her child's previously collected information and to refuse the further collection or use of a child's information and procedures for a parent's exercise of those rights.*

In its 2003 privacy guidance, OMB states that federal agencies should provide the name and contact information of the agency's representative who is required to respond to parents' inquiries about the website.

If your website is directed to children, place a link to the notice on your website's homepage and at each area on the website where personal information is collected from children.

If your general website is not directed to children but has a special children's area or site, place a link to the notice on the homepage of your website's children's area or site and at each area where children's information is collected.

- *OMB's 2003 privacy guidance for federal agencies requires this for agencies with websites that have a specific area or site for children and collect children's personal information.*

Make sure that the link to the notice of your practices regarding children's information is clearly labeled as such.

Obtaining Parental Consent:

Require verifiable parental consent for the collection, use and disclosure of children's personal information.

- *You may also consider requiring verifiable parental consent to a material change in your collection, use and/or disclosure practices to which a parent has previously consented.*
- *OMB's 2003 privacy guidance provides that a federal agency must send a notice of its information collection practices to a parent when the agency would like to obtain a parent's consent prior to the collection of a child's personal information.*

Provide a parent with the option to consent to the collection and use of his or her child's personal information without consenting to the disclosure of that information to third parties.

Ensure that notices to parents include:

- *Your desire to collect personal information from children*
- *The same information you post to your website regarding your information practices concerning the collection, use and/or disclosure of children's online information.*

OMB's 2003 privacy guidance provides that an agency's notice to a parent must inform the parent of the agency's wish to collect the child's personal information, that parental consent is required for the collection of such information, how a parent can provide consent, and either a link to or the information contained in the agency's privacy policy.

Establish exceptions for instances in which parental consent is not required in order to collect a child's information.

- *Examples of situations in which you might consider not requiring parental consent include collecting information for a one-time response to a child's inquiry or for providing information for law enforcement investigations.*
- *Children's activities that you might consider placing within an exception to requiring parental consent are for newsletters, homework help, contests and electronic postcards.*
- *More detailed information about these exceptions is included at the end of this section.*

Establish a "sliding scale" for methods of obtaining parental consent according to how a child's information will be used. For instances in which a child's information will not be disclosed to third parties, you may not need to use as stringent methods for obtaining a parent's consent.

- *OMB's 2003 privacy guidance utilizes the "sliding scale" approach for federal agencies.*

- *The FTC COPPA Final Rule uses the "sliding scale" approach as detailed above to verify a parent's consent. Originally, the approach was due to end or "sunset" in April 2002. However, because of the FTC's determination that secure electronic technology and infomediary services are not yet available at a reasonable cost, the FTC extended the end date for the sliding scale approach to April 21, 2005. Hence, if you use the "sliding scale" approach, you may want to place a time limit on it, depending upon when you anticipate that technology will mature to the point that more reliable methods of verification will be available.*
- *OMB's 2003 privacy guidance makes a distinction between private sector website operators' disclosure of children's personal information to third parties and such disclosures by federal agencies. It states that, generally, federal agencies only collect such information for immediate online activities or "other, disclosed, internal agency use." The internal use of children's personal information by federal agencies includes the "release to others who use it solely to provide support for internal operations of the site or service, including technical support and order fulfillment." However, federal agencies may not use children's information in a manner that was not initially disclosed or for which it has not received a parent's consent.*

For a child's information that will only be used internally by an agency, you may consider using email in combination with one of the following additional measures:

- *After you receive the parent's consent, providing a parent with a confirmation email*
- *Obtaining a parent's postal address or phone number in addition to his or her consent and calling or mailing the parent to confirm his or her consent.*

For a child's information that will be disclosed to third parties, you may consider using one of the following verification methods:

- *Sending a parent a consent form to be signed and returned via postal mail or fax*
- *Requiring that the parent use a credit card in connection with the transaction*
- *Requiring that a parent call a toll-free number staffed by trained personnel*
- *Using a digital certificate that utilizes public key technology*
- *Using email plus a PIN or password obtained through one of the above verification methods.*

A Note on Exceptions to Requiring Parental Consent:

The FTC's Final Rule on COPPA provides detailed provisions regarding exceptions to the parental consent requirement. Below are some additional instances in which you might consider providing an exception to obtaining a parent's consent with respect to the collection, use and/or disclosure of his or her child's information.

- **Informing Parents of Your Information Practices or Obtaining Parental Consent:** Where a child's or parent's name or online contact information is collected for the sole purpose of providing a notice of your information practices to a parent or obtaining parental consent (you may consider deleting the child's information if the parent does not consent within a reasonable time after the collection)
- **Providing a One-Time Response to a Child's Request:** Where a child's information is collected for the sole purpose of responding directly to a child's specific request on a one-time basis and the child's information is then deleted and not used to re-contact the child
- **Providing Multiple Responses to a Child's Request:** Where a child's online information is collected in order to be used for multiple responses to a child's specific request and the information is not used for any other purposes (in this case, you may consider making a reasonable effort immediately after the first response and before issuing additional responses to provide the parent, possibly through postal mail or an email message to the parent's email address, notice and an opportunity to decline the use of his or her child's information)
- **Protecting a Child Visiting Your Website:** Where a child's name and online contact information are collected to the extent reasonably necessary to protect a child visiting your website and you take reasonable steps to provide the parent with notice (in this instance, you may consider restricting use of the information for purposes other than protecting the child's safety and requiring that the information not be disclosed to third parties or to re-contact the child)
- **Safety and Law Enforcement-Related Exceptions:** Where a child's name and online contact information are used solely to the extent reasonably necessary to protect your website's security or integrity, take precautions against liability, respond to judicial process or to the extent otherwise permitted by law to provide information to law enforcement or for an investigation regarding a public safety matter.

If you choose to incorporate one or more of these exceptions, you might consider consulting §312.3 (c) of the COPPA Final Rule, since that provision deals with additional items of information you may want to include in any notices you provide to parents.

Considerations for the Use and Disclosure of Children's Personal Information:
Establish reasonable procedures to ensure the security, integrity, and confidentiality of children's personal information.

Enter into written agreements with any third parties to whom children's information may be disclosed to ensure its security, integrity, and confidentiality in the hands of those third parties.

Addressing the Privacy of Children's Information in Your Website Privacy Policy

Many states post website privacy policies online. Some address the privacy of children's information. Below is a list of elements regarding children's information that you may consider including in your state's website privacy policy along with the state examples for your reference.

Children's Privacy Issue	State	Link to State Privacy Policy
Whether your state mandates that agencies comply with COPPA's requirements: • Nevada and Arizona inform their website visitors that they have mandated that their agencies comply with COPPA's requirements if they knowingly collect information from children under the age of 13.	NV	http://psp.state.nv.us/IEM_POL_5.7.htm *(see §6.1.2 relating to the privacy of children's information)*
	AZ	http://www.az.gov/webapp/portal/displaycontent.jsp?name=privacy
Whether you can determine the age of a person volunteering information online or by email: • If you cannot determine the age of such persons, then you may consider stating so. Nevada takes this approach.	NV	http://psp.state.nv.us/IEM_POL_5.7.htm *(see §6.1.2 relating to the privacy of children's information)*
Whether the information submitted by children will be treated the same as that submitted by adults and whether it may be subject to public access: • Both Nevada and Colorado provide a statement to this effect in their website privacy policies.	NV	http://psp.state.nv.us/IEM_POL_5.7.htm *(see §6.1.2 relating to the privacy of children's information)*
	CO	http://www.colorado.gov/about_this_website.html#privacy
Whether the website is directed to children under the age of 13: • Indiana's website privacy policy states that the accessIndiana portal is not directed to children under the age of 13.	IN	http:// www.in.gov/ai/policies/privacy.html

Children's Privacy Issue	State	Link to State Privacy Policy
Whether the website sells products or services for purchase by children: • Indiana's website privacy policy states that it does not sell products or services for purchase by children.	IN	http://www.in.gov/ai/policies/privacy.html
Whether there is a state webpage for children: • New Jersey states in its general website privacy notice that it has a webpage for children that encourages them to send email messages with feedback and suggestions. The privacy notice goes on to state that "We specifically ask children to get their parents' permission before providing any information online—at our site or any other site—and hope parents will always be involved in those decisions. Most importantly, when children do provide information through the State of New Jersey website, it is only used to enable us to respond to the writer, and not to create profiles of children."	NJ	http://www.state.nj.us/privacy.html
Provide a contact person for parents with questions: • Virginia's website privacy policy states that, if information is collected from a child, a parent can contact the state for more about what information is collected and options available under COPPA.	VA	http://www.myvirginia.org/cmsportal/vipnet_987/policy_1112/index.html #privacy

The FTC's "Kidz' Privacy Website" contains information about how children can safely surf the web. You may consider placing a link to that website on your state website. View the FTC's "Kidz' Privacy" website at: http://www.ftc.gov/bcp/conline/edcams/kidzprivacy/.

State Department of Motor Vehicles Information ::

Important Information Privacy Issue

An issue of importance to the states is protecting the personally identifiable information that is contained in records maintained by state Departments of Motor Vehicles (state DMVs). State DMVs collect personal information from individuals when performing a variety of tasks, including issuing driver's licenses. This has raised the issue of when and to whom state DMVs can disclose personal information.

Federal Authority on the Issue

The Driver's Privacy Protection Act of 1994 (DPPA), 18 USC §§2721-2725.

- **What Does It Do?** The DPPA restricts the disclosure of personal information obtained by state DMVs in connection with the motor vehicle records they keep. The DPPA was enacted by Congress in response to the murder of actress Rebecca Shaeffer, whose killer obtained her address from a state DMV.

  The DPPA classifies certain types of information as "personal information," such as an individual's name, address and phone number. It restricts the disclosure of that information unless its disclosure falls within one of the DPPA's four enumerated exceptions. In 2000, Congress amended the DPPA to classify an individual's photo, Social Security Number, and medical or disability information as "highly restricted" information that can only be disclosed without an individual's express consent in four enumerated instances.

  The DPPA also makes it illegal for a person to knowingly obtain or disclose personal information contained in a motor vehicle record for any purpose that is not otherwise permitted in the statute.

  Finally, the DPPA prohibits making false representations to obtain personal information from a motor vehicle record.

- **To Whom Does It Apply?** The DPPA applies to state DMVs and their officers, employees and contractors. However, the DPPA's prohibitions on obtaining, disclosing, or making false representations to obtain the personal information in motor vehicle records apply to any person, including an individual, organization or entity. Note that the DPPA's prohibitions do not apply to a state or an agency of a state.

- **What Elements of Control Do States Have Regarding State DMV Information?** While this federal law directly regulates state DMVs' disclosure of information contained in motor vehicle records, states, at their discretion, can provide for additional privacy protections for motor vehicle records. The DPPA also specifically provides that it does not prohibit states from charging an administrative fee for the issuance of motor vehicle records.

Link to the DPPA: http://www4.law.cornell.edu/uscode/18/pIch123.html.

Application of this Privacy Issue

What Types of State DMV Information are Involved in this Issue? The DPPA applies to a motor vehicle record, which is "any record that pertains to a motor vehicle operator's permit, motor vehicle title, motor vehicle registration, or identification card issued by a department of motor vehicles." It restricts the disclosure of personally identifying information contained in those records, including a person's:

- Photograph
- Social Security Number
- Driver identification number
- Name
- Address (excluding the five-digit zip code)
- Telephone number
- Medical or disability information.

However, the DPPA does not include within its definition of "personal information" information on vehicular accidents, driving violations or a driver's status.

What Types of Activities are Involved in this Issue? If you are an officer, employee or contractor of a state DMV and are engaged in activities that might result in the disclosure of personal information contained in a motor vehicle record, such as a driver's license, permit or other identification card or a motor vehicle title or registration, you should be familiar with the disclosure restrictions and exceptions of the DPPA.

Furthermore, persons who are in a position to obtain and/or disclose personal information from motor vehicle records should be sure that their activities are compliant with the DPPA.

Considerations for Addressing the Privacy of State DMV Information

The DPPA directly applies to state DMVs as detailed above. Some of the considerations below are legally required by the DPPA. Where this is the case, it is noted. For any state DMVs that have a policy or practice of substantial noncompliance with the DPPA, the Attorney General may assess against the state DMV a civil penalty of not more than $5,000 per day for each day of substantial noncompliance. Persons, which includes individuals and entities, may also be criminally fined for knowingly violating the DPPA. An individual whose information was disclosed or used in violation of the DPPA may bring a civil action against DPPA violators in United States District Court. A court may award any or all of the following remedies:

- *Actual damages (but not less than liquidated damages of $2,500)*
- *Punitive damages where the conduct is a willful or reckless disregard of the law*
- *Reasonable attorneys' fees and litigation costs*
- *Other preliminary and equitable relief that the court finds to be appropriate.*

Collecting Personal Information:

Establish a policy for what types of information are collected and whether the collection of such information is legally required or discretionary.

Establish what types of information an individual may refuse to divulge and still receive a driver's license or other document.

Disclosure Restrictions and Exceptions for Personal Information:

If you, as a state DMV, collect personal information from individuals in connection with a motor vehicle record, then the DPPA restricts your disclosure of the following types of personal information:

- *Photograph*
- *Social Security Number*
- *Driver identification number*
- *Name*
- *Address (excluding the five-digit zip code)*
- *Telephone number*
- *Medical or disability information.*

If another person or entity requests the disclosure of personal information obtained by you in connection with a motor vehicle record, you must under the DPPA obtain the "express consent" of the individual to whom the information pertains in order to disclose that information to another person or entity.

- *An individual's "express consent" means that an individual's consent to the disclosure of his or her personal information is in writing or conveyed electronically so that it bears an electronic signature.*
- *An individual requestor of personal information may obtain the information for any use if he or she demonstrates that he or she has obtained the written consent of the individual to whom the personal information pertains.*
- *A state DMV may not place a condition upon the issuance of a motor vehicle record that would require an individual to grant his or her express consent to the further disclosure of his or her personal information.*

There are exceptions under which you can disclose the personal information you obtained in connection with a motor vehicle record without an individual's consent. These exceptions as enumerated in the DPPA are:

- *For use by any government agency in carrying out its functions*
- *For use in matters of motor vehicle safety or driver safety and theft*
- *In connection with legal proceedings*
- *For use in research activities and statistical reports*
- *For use by insurers in underwriting and claims investigations*
- *To provide notice to the owner of an impounded or towed vehicle*
- *To licensed private investigators or licensed security services*
- *To employers to verify information about the holder of a commercial driver's license*
- *For use in the operation of private toll transportation facilities*
- *For any other use specifically authorized by your state's law if the use is related to the operation of motor vehicles or public safety.*

If a business requests the disclosure of personal information, then in accordance with the DPPA you may disclose that information to the business, provided that the following requirements are satisfied:

- *The business is "legitimate" (note that the DPPA does not further define the term "legitimate")*
- *The personal information is for use within the normal course of business*
- *The personal information is only used to verify the accuracy of personal information submitted to the business by an individual or, if the submitted information is incorrect,*

to obtain the correct information only for purposes of preventing fraud by, pursuing legal remedies against, or recovering a debt or security interest, against the individual.

If personal information is requested for purposes of a bulk distribution for surveys, marketing or solicitations, under the DPPA, you may disclose an individual's personal information if the individual provides you with his or her express consent.

For authorized recipients of personal information, the DPPA specifies that those recipients can generally redisclose or resell that personal information, as long as the redisclosure or resale is for uses permitted by the DPPA. However, be sure to note two exceptions contained in the DPPA:

- *If the state has the express consent of the individual to disclose personal information, then the recipient of the information may redisclose or resell it for any purpose.*
- *If a state discloses personal information with the express consent of the individual for a bulk distribution for surveys, marketing or solicitations, the recipient of the personal information may only redisclose or resell it under the DPPA exception for disclosures for bulk surveys, marketing or solicitations.*

You may choose to require those who obtain the personal information (or "highly restricted personal information," which is discussed below) of another person to sign under penalty of false statement that the information will only be used for the purposes specified in the DPPA and any other applicable state laws. Note that the signing of this type of statement does not appear to be a requirement of the DPPA.

Under the DPPA, you may establish procedures to deal with requests for information that do not fall within the DPPA's exceptions for disclosing an individual's personal information.

- *The DPPA specifies that the procedures should allow the state DMV to mail a copy of the request to the individual whose personal information has been requested. The notice should inform the individual that the information was requested, and include a statement that the information will not be disclosed unless the individual waives his or her privacy rights under the DPPA.*

Disclosure Restrictions and Exceptions for "Highly Restricted Personal Information":

If you collect the following types of information in connection with a motor vehicle record, the DPPA classifies those types of information as "highly restricted personal information":

- *An individual's photo or image*
- *Social Security Number*
- *Medical or disability information.*

If you collect "highly restricted personal information," you generally cannot, under the DPPA, disclose it without the express consent of the individual.

According to the DPPA, you may only disclose "highly restricted personal information" without the consent of the individual in the following four instances:

- *For use by any government agency in carrying out its functions*
- *In connection with legal proceedings*
- *For use by insurers in underwriting and claims investigations*
- *For use by employers to verify information about the holder of a commercial license.*

Other Considerations:
You may consider establishing a process through which a person can correct his or her personal information if it is incorrect.

Under the DPPA, a state DMV can charge an administrative fee for the issuance of a motor vehicle record.

Addressing the Privacy of State DMV Information on Your State's DMV Website

States may post to their DMV websites information on the handling of individuals' personal information. Below is a list of elements you may consider including on your state DMV's website and state examples of those elements.

Driver's Privacy Issue	State	Link to State DMV Privacy Policy
What types of personal information are collected by the state DMV: • You may choose to specify the types of personal information the state DMV is required to collect and the law or regulation that requires the collection. You may also specify whether the refusal of certain types of personal information can result in the refusal or revocation of a motor vehicle record, such as a driver's license.	CA	http://www.dmv.ca.gov/dl/authority.htm
Whether Social Security Numbers (SSNs) are required to be collected by the state DMV: • You may state whether any SSNs that are collected will appear on an individual's motor vehicle record, such as on the face of a driver's license or encoded into a driver license's magnetic stripe, and to whom SSNs may be disclosed. If a motor vehicle record will list a SSN, you may state whether it will be masked or blacked-out if the motor vehicle record is disclosed.	CA	http://www.dmv.ca.gov/dl/authority.htm *(see section on Social Security Numbers)* http://www.dmv.ca.gov/dl/dl_info.htm#SSN
Explain the requirements of the DPPA: • You may explain in detail under what circumstances an individual's personal information may be disclosed.	CT CA FL IA	http://www.ct.gov/dmv/cwp/view.asp?a=809&Q=244636&dmvPNavCtr=|#3082. http://www.dmv.ca.gov/dl/authority.htm. http://www.hsmv.state.fl.us/ddl/dppa.html. http://www.dot.state.ia.us/mvd/ods/licapp.htm#Privacy%20of%20Driver's%20License%20or%20ID%20Information.

Driver's Privacy Issue	State	Link to State DMV Privacy Policy
Whether there are circumstances under which an individual should receive a notice of a request for his or her personal information: • You may include whether the individual who receives such a notice will have the opportunity to refuse the disclosure of his or her personal information.	CA	http://www.dmv.ca.gov/dl/authority.htm
Whether there are specific rules that apply to the disclosure of public officials' personal information: • For example, you may explain whether and under what circumstances the residential addresses of public officials, such as judges and police officers, may be released to another individual.	CA	http://www.dmv.ca.gov/dl/authority.htm
Whether a person must sign a form stating that they will use another individual's personal information that has been disclosed to him or her according to any applicable legal requirements: • If the recipient of another's information must sign such a statement, you may specify the penalty for a recipient's noncompliance.	CT	http://www.ct.gov/dmv/cwp/view.asp?a=809&Q=244636&dmvPNavCtr=|#3082
Whether there is a process for an individual to correct his or her personal information if he or she discovers it is incorrect: • If such a process is in place, you may provide details about the process.	CA	http://www.dmv.ca.gov/dl/authority.htm
If your state allows for online DMV transactions, such as driver's license renewals, explain the types of information that may be collected and how it might be used: • Your state DMV may include this information in its more general website privacy policy. You also can list details about the DPPA in your state DMV's website privacy policy.	NY	http://www.nydmv.state.ny.us/securitylocal.htm

Health Information ::

Important Information Privacy Issue

An issue of importance for states and other entities is protecting individuals' personal health information. Both public and private entities, including hospitals, doctors' offices, and health care information clearinghouses, handle individuals' personal health-related information. This has raised questions about how an individual's health information may be used by such entities and when and how it can be disclosed to others. Another issue of importance is when and how an individual can access his or her own health information for review and correction, if necessary.

Federal Authority on the Issue

Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191 (1996).

- **What Does It Do?** Congress enacted HIPAA to standardize the electronic exchange of health information and to improve the privacy and security of health information. HIPAA also authorized the Secretary of Health and Human Services (HHS) to issue rules to accomplish its purpose. To that end, the Secretary of HHS promulgated the HIPAA rules on a phased-in basis. Many of the rules, such as the Transactions and Code Sets Rule, the Privacy Rule, and the Security Rule, have been issued in their final form. The general purpose of each rule is as follows:

  - **The Privacy Rule:** This rule provides privacy protections for individually identifiable health information by regulating its use and disclosure by entities covered by HIPAA.

    The compliance deadline for the Privacy Rule was April 14, 2003 (note that, for small health plans, the deadline is April 14, 2004).

  - **The Security Rule:** This rule standardizes the way that entities covered by HIPAA protect the confidentiality, integrity, and availability of electronic protected health information. It protects such information while held by an entity regulated by HIPAA and also while in transit.

    The compliance deadline for the Security Rule is April 21, 2005 (note that, for small health plans, the deadline is April 21, 2006).

  - **The Transactions and Code Sets Rule:** For entities covered by HIPAA, this rule standardizes data content by specifying uniform definitions of the data elements that will be exchanged in electronic transactions and identifies the specific codes or values that are valid for each data element.

    The compliance deadline for the Transactions and Code Sets Rule was October 16, 2002 (note that, for small health plans and covered entities that filed a compliance plan with HHS before October 16, 2002, the deadline was October 16, 2003).

- **To Whom Does It Apply?** HIPAA applies to health plans, health care clearinghouses, and health care providers who transmit health information electronically. Such entities are called "covered entities." Because some state government agencies handle health information, such agencies have had to determine if they are a "covered entity" as defined by HIPAA. If so, those state agencies have had to develop and implement HIPAA's provisions and rules.

- **What Elements of Control Do States Have Regarding Health Information?** HIPAA's Privacy Rule leaves intact state medical privacy laws that are more stringent in their privacy protections than HIPAA. However, the Privacy Rule provides that HIPAA preempts provisions of state laws that are contrary to the Privacy Rule's provisions. Exceptions apply in certain situations, such as where a state law provides for the reporting of disease, injury, child abuse, birth or death. The Privacy Rule also provides a process for states to request an exception from the Secretary of HHS regarding the preemption of state law.

Link to HIPAA: http://hipaadvisory.com/regs/law/index.htm.

Link to the Privacy Rule: http://www.os.dhhs.gov/ocr/combinedregtext.pdf.

Link to the Security Rule: http://www.hipaadvisory.com/regs/Regs_in_PDF/finalsecurity.pdf.

Link to the Transactions and Code Sets Rule: http://www.hipaadvisory.com/regs/Regs_in_PDF/finaltrans.pdf.

Application of this Privacy Issue

What Types of Health Information are Involved in this Issue? The HIPAA Privacy Rule applies to individually identifiable health information that is used or disclosed by HIPAA covered entities. However, one notable exception is protected health information that is contained in a student's educational records. Such information is not subject to HIPAA as long as it is protected by the Family Educational Rights and Privacy Act (FERPA).

What Types of Activities are Involved in this Issue? It is important to note that the Privacy Rule applies not only to protected health information that is held by a covered entity in an electronic form but also to such information held in paper form or transmitted orally. Another notable aspect of the Privacy Rule is that it recognizes that there may be instances in which only certain parts of a covered entity's business activities are covered by HIPAA. In such cases, the Privacy Rule allows a covered entity to designate itself as a "hybrid entity." For a hybrid entity, HIPAA's requirements only apply to certain designated portions of the hybrid entity.

Considerations for Addressing the Privacy of Health Information

The following considerations are for entities covered by HIPAA. For those entities not covered by HIPAA, they may follow HIPAA's requirements as a guide to improving the overall privacy of any health-related information that they may handle.

Hybrid Entities:

If you meet the following requirements, then you are a hybrid entity:

- *You are a covered entity*
- *Your business activities include both covered and non-covered functions (note that a covered function is a function that your entity performs that makes it qualify as a HIPAA covered entity)*
- *You designate health care components, which are components to which HIPAA's requirements apply.*

If you are a hybrid entity, then you must do the following when designating your health care components:

- *Designate the components that are part of one or more health care components you designate*
- *Document your designations*
- *Include within your designation of a health care component any component that would meet the definition of a covered entity if that component were a separate legal entity*
- *Include components in your health care components only to the extent that they perform:*
    - *Covered functions under HIPAA or*
    - *Activities that would make them a business associate of a component that performs covered functions if the two components were separate legal entities.*

If you are a hybrid entity, HIPAA's requirements regarding privacy only apply to your health care components.

In making sure that your designated health care components comply with the HIPAA Privacy Rule, you must ensure that:

- ***For a health care component:*** *That it does not disclose protected health information to another component if that disclosure would be prohibited if the two components were separate legal entities*
- ***For a person who performs duties for both your health care components and other components:*** *That he or she does not use or disclose protected health information created or received during his or her work for the health care component in a way that violates the Privacy Rule*
- ***For a component that would be a business associate of another component that performs covered functions if the two components were separate and distinct legal entities:*** *That the component does not use or disclose protected health information it creates or receives from a health care component in a way that violates the Privacy Rule.*

Patient Consent for the Use and Disclosure of Protected Health Information:

For routine uses and disclosures of protected health information, you may, at your discretion, obtain a patient's consent (in other words, patient consent for routine uses and disclosures is optional under HIPAA's Privacy Rule). Routine uses of protected health information are:

- *For treatment of a patient*
- *For payment activities*
- *For health care operations.*

For non-routine uses and disclosures of protected health information, you must obtain a patient's consent (such as for marketing purposes).

- *For non-routine uses, covered entities can use one type of authorization form to obtain a patient's consent. The Privacy Rule specifies the elements that an authorization must include in order to be valid.*
- *The patient must complete a separate authorization form for each type of non-routine use or disclosure of his or her protected health information, except in certain instances specified in the Privacy Rule.*

An Individual's Right to Restrict the Use and Disclosure of Protected Health Information:

Allow an individual to request that you, as a covered entity, restrict:

- *Uses and disclosures of protected health information to carry out treatment, payment or health care operations*
- *Disclosures otherwise permitted under the Privacy Rule to others who are involved in an individual's care, such as family members.*

As a covered entity, you are not required by the Privacy Rule to agree to the above-listed types of restrictions that an individual has a right to request.

If you do agree to such a restriction, you may not use that individual's protected health information in violation of the restriction unless the individual who requested the restriction is in need of emergency treatment and the restricted protected health information is needed to provide the emergency treatment.

Notice of a Covered Entity's Privacy Practices and Patient Privacy Rights:

Provide patients with a written copy of your privacy practices and a notice of patient privacy rights.

- *The Privacy Rule requires that covered entities provide this privacy notice upon an individual's request. There are exceptions for when a group health plan or a correctional institution that is a covered entity must provide notice. The Privacy Rule also contains specific information about when health plans must provide individuals covered by their plans with the notice and when health care providers must provide such notices to their patients.*
- *Covered entities must promptly revise and distribute their notices whenever there has been a material change in their use and disclosure of health information or a material change to an individual's rights, the covered entity's legal duties or other privacy practices detailed in the notices.*

Make sure that your privacy notice contains the following items that are mandatory under the HIPAA Privacy Rule:

- *A header stating: "THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY."*
- *Information on the use and disclosure of individuals' health information*
- *Individuals' rights regarding their protected health information and how individuals may exercise their rights*
- *The covered entity's duties with respect to privacy notices*
- *A statement that individuals may complain to the covered entity or the Secretary of HHS if they believe that their privacy rights have been violated, how to file a complaint with the covered entity, and a statement that the covered entity will not retaliate against individuals for filing a complaint.*

- *A person to contact for more information about uses and disclosures of protected health information*
- *The effective date of the notice.*

If you elect to limit uses or disclosures of protected health information as permitted under the Privacy Rule, you may describe those limitations in your privacy notice.

If you maintain a website that has information about your customer services or benefits, you must post in a prominent place your privacy notice on your website and make the notice available electronically via your website.

You also may provide an individual with notice of your privacy practices via email if the individual agreed to such an electronic notice.

- *When provided in accordance with the Privacy Rule's other provisions, you can satisfy the Privacy Rule's notice requirements by sending your privacy notice electronically.*
- *The Privacy Rule details additional provisions on how covered entities can provide notice via email.*

Make a good faith effort to obtain a patient's written acknowledgment of receipt of the privacy notice if you are a covered health care provider who has a direct treatment relationship with the individual.

- *The Privacy Rule provides an exception to this requirement in emergency treatment situations.*
- *If a covered entity cannot obtain a written acknowledgment of the receipt of the notice, the covered entity must document its good faith efforts to obtain the acknowledgment and the reason why the acknowledgment was not obtained.*

Document your compliance with the Privacy Rule's notice requirements by:

- *Retaining copies of the notices you issue*
- *If you must make a good faith effort to obtain a patient's written acknowledgment of your privacy notice, retain copies of any written acknowledgments or documentation of your good faith efforts.*

Minimum Amount Necessary Limitation:

When you use or disclose protected health information or request such information from another covered entity, you must make reasonable efforts to limit the protected health information to the minimum amount necessary to accomplish the intended purpose of your use, disclosure or request. However, there are exceptions to this general rule, which include:

- *Disclosures to or requests by a health care provider for treatment*
- *Uses or disclosures to the individual that are permitted or required by the Privacy Rule*
- *Uses or disclosures that are authorized by an individual*
- *Disclosures made to the Secretary of HHS in accordance with the Privacy Rule*
- *Uses or disclosures that are required by law*
- *Uses or disclosures that are required in order to comply with the Privacy Rule.*

Use and Disclosure of Protected Health Information:

If you use or disclose protected health information, make sure such uses are permitted under the HIPAA Privacy Rule. Permitted uses or disclosures include:

- *To an individual*
- *For treatment, payment or health care operations (patient consent is optional)*
- *Incident to a use or disclosure that is otherwise permitted by the Privacy Rule (as long as you comply with the minimum necessary limitation and training requirements for your workforce)*
- *Under an authorization that complies with the Privacy Rule's authorization requirements*
- *Under an agreement or other permitted use or disclosure for a facilities directory or to those involved in an individual's care or payment, such as family members*
- *Where the Privacy Rule permits uses and disclosures without an authorization or opportunity to agree or object, such as for specified public health purposes.*

Make sure that you disclose protected health information where required by the Privacy Rule in the following instances:

- *To an individual under the Privacy Rule's provisions that deal with individuals' access to their protected health information and their right to an accounting of disclosures of their protected health information*
- *As required by the Secretary of HHS to investigate or determine a covered entity's compliance with the Privacy Rule.*

Identifying Business Associates:

Determine whether other persons or entities that work with you perform functions, activities or services for you that could make them a business associate.

- *Note, though, that functions, activities or services performed for you by a member of your workforce do not make members of your workforce business associates.*

If a person or entity performs or assists in performing activities or functions for you that include the use or disclosure of individually identifiable health information for you, they may be a business associate. Such functions or activities include:

- *Claims processing or administration*
- *Data analysis*
- *Processing or administration*
- *Utilization review*
- *Quality assurance*
- *Billing*
- *Benefit management*
- *Practice management*
- *Repricing, or*
- *Any other function or activity that would be regulated by HIPAA's Privacy Rule.*

If persons or entities provide the following types of services for or to you that involve the disclosure of individually identifiable health information by you or another business associate of yours, those persons or entities may be business associates:

- *Legal*
- *Actuarial*
- *Accounting*
- *Consulting*
- *Data aggregation*

- *Management*
- *Administrative*
- *Accreditation*
- *Financial services.*

If you are a covered entity that participates in an organized health care arrangement, you need to be aware that, just because you perform functions, activities or services as described above for or on behalf of the organized health care arrangement, you do not necessarily become a business associate of the covered entities that participate in the organized health care arrangement.

- *Review the Privacy Rule definitions if you have questions about whether you participate in an organized health care arrangement.*

Even if you are a covered entity, you may still qualify as a business associate of another covered entity.

Sharing Protected Health Information with Business Associates:

If you are a covered entity, you may disclose protected health information to your business associates and may allow them to create or receive protected health information on your behalf as long as you obtain satisfactory assurances that your business associates will appropriately safeguard the protected health information. Exceptions to this provision of the Privacy Rule include:

- *Disclosures you make as a covered entity to a health care provider concerning an individual's treatment*
- *Disclosures or uses by a health plan that is a government program providing public benefits in the following situations where the collection and sharing of individually identifiable information is authorized by law:*
  - ⇨ *If eligibility for or enrollment in the health plan is determined by an agency other than the agency administering the health plan, or*
  - ⇨ *If the protected health information used to determine enrollment or eligibility in the health plan is collected by an agency other than the agency administering the health plan.*

In order to share information with your business associates, you must document the satisfactory assurances of your business associates concerning the safeguarding of information through a written contract or agreement. Contracts or agreements with business associates must include the following elements:

- *The permitted and required uses and disclosures of protected health information by the business associate (note, with a few exceptions, that the contract cannot authorize uses or disclosures by the business associate that, if performed by the covered entity, would violate the Privacy Rule)*
- *That the business associate will not use or further disclose the information other than as permitted by the contract or as required by law*
- *That the business associate will use the appropriate safeguards to prevent uses or disclosures other than those provided by the contract*
- *That the business associate will report to the covered entity any uses or disclosures that are not provided for in the contract*
- *That the business associate will ensure that agents, including subcontractors, to whom it provides protected health information will agree to the same conditions and restrictions*

- *That the business associate will make available to individuals protected health information in accordance with the Privacy Rule's access, amendment and accounting of disclosure provisions*
- *That the business associate will make any amendments requested in accordance with the Privacy Rule's amendment provisions*
- *That the business associate will make its internal practices, books and records relating to the use and disclosure of protected health information available to the Secretary of HHS for purposes of determining the covered entity's compliance*
- *That, upon termination of the contract, the business associate will return to the covered entity or destroy the protected health information or, if that is not feasible, make the contract extend protection to the information and limit the use and disclosure of it to those purposes that make its return or destruction infeasible*
- *Authorization for the covered entity to terminate the contract if the business associate has violated a material term of the contract.*

If both you and your business associate are governmental entities, you may comply with the Privacy Rule's requirements regarding the content of your business associate agreement:

- *By entering into a memorandum of understanding with the business associate that accomplishes the objectives of the Privacy Rule's provisions on the content of business associate agreements*
- *If other law, including regulations adopted by you or the business associate, accomplishes the objectives of the Privacy Rule's provisions on the content of business associate agreements.*

If you, a covered entity, violate the satisfactory assurances you provided as a business associate of another covered entity, you will not be in compliance with the Privacy Rule.

You also will not be in compliance with the Privacy Rule as a covered entity, if you knew of a pattern of a business associate's material breach of your agreement, unless you took reasonable steps to remedy the breach or end the violation and, if such steps were unsuccessful, you terminated the contract, if feasible, or, if not feasible, reported the situation to the Secretary of HHS.

Individual Access Rights to Protected Health Information (Including Parental Access Rights):

Allow for an individual to inspect and obtain a copy of his or her protected health information. Exceptions to this right of access include:

- *Psychotherapy notes*
- *Information compiled in reasonable anticipation of or use in legal proceedings*
- *Protected health information subject to certain provisions of the Clinical Laboratory Improvements Amendments of 1988.*

The Privacy Rule specifies instances in which a covered entity may deny an individual access to his or her protected health information.

- *These exceptions to the Privacy Rule's access right provisions are grouped within the Privacy Rule according to whether the covered entity's denial of access may be reviewed by another licensed health care professional who was designated by the covered entity as a reviewing official and who did not participate in the original denial.*

Instances in which you, as a covered entity, can deny an individual a right of access to his or her protected information without an opportunity to have that decision reviewed include:

- *If the information is otherwise exempted from a right of access by the Privacy Rule (for example, the Privacy Rule exempts psychotherapy notes from the right of access)*
- *If the covered entity is a correctional institution or a covered health care provider acting under the direction of a correctional institution where there are safety-related concerns in disclosing the information to an inmate*
- *If the covered health care provider obtained or created the information during the course of research that included treatment as long as the covered entity fulfilled certain requirements stated in the Privacy Rule*
- *If the information is contained in records subject to the Privacy Act of 1974 and the denial of access would meet the requirements of that federal law*
- *If a person other than a health care provider obtained the protected health information under a promise of confidentiality and allowing access to the information would be reasonably likely to reveal the source of the information.*

Instances in which you can deny an individual a right of access to his or her protected health information with an opportunity to have the denial reviewed include situations in which a licensed health care professional, in the exercise of professional judgment, determines that access would be reasonably likely to:

- *Endanger the life or safety of the individual or another person*
- *Cause substantial harm to another person referenced within the protected health information (unless the other person is a licensed health care provider)*
- *Cause substantial harm to the individual or another person, if an individual's personal representative would be provided access.*

Generally, you must act on a request from an individual to view his or her protected health information within 30 days after the receipt of the request.

- *If the requested protected health information is not accessible or maintained by a covered entity on-site, then the covered entity must act on the request no later than 60 days after the receipt of the request*
- *If a covered entity cannot act on an individual's request within the timeframes discussed above, it can extend the time period to act by no more than 30 days if the covered entity notifies the individual within the original timeframe of the delay, the reason for the delay and a date by which the covered entity will act on the request (a covered entity may only have a one-time extension for each request).*

The Privacy Rule contains provisions and other details regarding:

- *When and how a covered entity must comply with its duty to provide individuals access to their protected health information*
- *When and how a covered entity may deny an individual's right of access*
- *When and how a covered entity may review a denial of an individual's right of access*
- *Documentation requirements related to an individual's right of access.*

If you are dealing with an issue of whether to release the protected health information of a child to the child's parent or legal guardian, then the Privacy Rule grants the parent or legal guardian a general access right. However, regarding state laws on the disclosure of such information, the following rules apply:

- *If a state law specifically permits the disclosure of a child's records in a particular situation, you may disclose that information accordingly.*
- *If a state law specifically prohibits the disclosure of a child's records in a particular situation, you may not disclose that information.*
- *If state law is silent as to whether the disclosure of a child's protected health information is permitted in a specific instance and the Privacy Rule does not specifically grant a parent or legal guardian a right of access, a licensed health care professional, exercising his or her professional judgment, may permit or deny access, as long as the decision is consistent with state or other applicable law.*

Individual Amendment Rights :

You must allow an individual the right to have you amend his or her protected health information.

- *The Privacy Rule contains several exceptions under which you may deny an individual's request including if the information is already complete and accurate or if the information would not be available for the individual's inspection under the Privacy Rule's individual access rights provisions.*

Generally, you must act on an individual's request for an amendment within 60 days after the receipt of the request.

- *If you are unable to act on such an amendment request within 60 days, you can extend the time period by 30 days as long as you provide the individual with a written statement regarding the delay, the reasons for the delay and the date by which you will provide action on the request.*
- *You can only have one extension of time for action on an amendment request.*

The Privacy Rule also contains provisions and other details regarding:

- *Making an amendment*
- *Informing the requesting individual of the amendment*
- *Informing others of an amendment that has been made*
- *Denying an amendment request*
- *Documentation requirements related to amending protected health information.*

Individual Accounting Rights:

At an individual's request, you must provide the individual with an accounting or listing of disclosures of protected health information made by you in the six years prior to the date of the individual's request. However, exceptions to this general right to an accounting include disclosures:

- *To carry out treatment, payment or health care operations*
- *To individuals of protected health information about them*
- *Incident to a use or disclosure otherwise permitted by the Privacy Rule*
- *Pursuant to an authorization*
- *For a facility's directory or to persons involved in an individual's care or other notification purposes*
- *For national security or intelligence purposes*
- *To correctional institutions or law enforcement officials*
- *As part of a limited data set*
- *That occurred prior to the covered entity's compliance date.*

You must act on an individual's request for an accounting of disclosures within 60 days of the date of the request.

- *If you are unable to provide such an accounting within 60 days, you can extend the time period for providing the accounting by 30 days as long as you provide the individual with a written statement regarding the delay, the reasons for the delay, and the date by which you will provide the accounting.*
- *You can only have one extension of time for action on an accounting of disclosures request.*

The Privacy Rule contains provisions and other details regarding:

- *The content of an accounting*
- *A covered entity's duty to temporarily suspend an individual's right to receive an accounting of certain disclosures to a health oversight agency or law enforcement official, if the health oversight agency or law enforcement official provides the covered entity with a written statement that the accounting would be reasonably likely to impede the agency's activities and that provides a time for which the suspension is required*
- *Documentation requirements related to an individual's right to an accounting of disclosures of protected health information.*

Ensuring Compliance and Privacy Training:

As a covered entity, you must designate a privacy official who has responsibility for the development and implementation of your privacy policies and procedures. Note that you must document this designation.

You must designate a contact person or an office that is responsible for receiving complaints regarding HIPAA Privacy Rule compliance and who is able to provide more information on the privacy notice that a covered entity must provide regarding its privacy policies and practices. Note that you must document this designation.

Establish and implement policies and procedures in a written or electronic form designed to comply with the Privacy Rule's provisions regarding protected health information.

Provide training for all members of your workforce on your policies and procedures regarding protected health information.

- *You must have provided training for each member of your workforce by the compliance date as stated in the Privacy Rule (April 14, 2003).*
- *After the Privacy Rule's deadline for compliance, you must provide training to each new member of your workforce within a reasonable period of time after a person joins your workforce.*
- *You must provide training to each member of your workforce whose functions are affected by a material change in your privacy policies or procedures within a reasonable period of time after the change becomes effective.*

Note that you must document your training of members of your workforce.

Enforcement of the Privacy Rule:

The HIPAA Privacy Rule lists as its "principles for achieving compliance" the following:

- ***Cooperation:*** *The Secretary of HHS will, to the extent practicable, seek covered entities'*

cooperation in obtaining compliance with the Privacy Rule.

- ***Assistance:*** *The Secretary of HHS may provide technical assistance to covered entities to help them voluntarily comply with the Privacy Rule.*

The Secretary of HHS has the authority to conduct compliance reviews to determine whether a covered entity is in compliance with the Privacy Rule.

The Privacy Rule lists as a covered entity's responsibilities the following:

- *Providing such records and compliance reports as the Secretary of HHS determines to be necessary to allow him to ascertain a covered entity's compliance*
- *Cooperating with complaint investigations and compliance reviews*
- *Permitting the Secretary of HHS access to information pertinent to determining a covered entity's compliance.*

Extent of HIPAA's Preemption of State Privacy Laws:

NOTE: The HIPAA Privacy Rule's preemption provisions refer to the preemption of a "state law." However, under the Privacy Rule's definitions, any reference to a "state law" encompasses "a constitution, statute, regulation, rule, common law, or other State action having the force and effect of law."

If your state has a health privacy law that is contrary to a HIPAA standard, requirement, or implementation specification, HIPAA preempts the contrary provisions of that state law.

- *A* ***"contrary"*** *state law under the HIPAA Privacy Rule means that "[a] covered entity would find it impossible to comply with both the State and federal requirements" or the state law "stands as an obstacle to the accomplishment and execution of the full purposes and objectives" of the administration simplification provisions of HIPAA or HIPAA's privacy provisions.*

If your state has a law that is more stringent than HIPAA in protecting the privacy of individually identifiable health information, HIPAA does not preempt that state law.

- *A* ***"more stringent"*** *state law under the HIPAA Privacy Rule means that a state law meets one or more of the following criteria:*
  - ⇨ *The state law prohibits or restricts a use or disclosure in circumstances under which such use or disclosure otherwise would be permitted by the HIPAA Privacy Rule (unless the disclosure is required by the Secretary of HHS in determining if a covered entity is in compliance with the Privacy Rule or if the disclosure is to the individual who is the subject of the individually identifiable health information)*
  - ⇨ *It provides individuals greater rights of access or amendment regarding their individually identifiable health information*
  - ⇨ *It provides a greater amount of information to individuals about a use, disclosure, right or remedy regarding their individually identifiable health information*
  - ⇨ *It narrows the scope or duration, increases privacy protections or reduces the coercive effect of the circumstances surrounding obtaining the express legal permission from an individual to disclose his or her individually identifiable health information*
  - ⇨ *Regarding recordkeeping or accounting of disclosures, it provides for the retention or reporting of more detailed information or for a longer duration*
  - ⇨ *It provides greater privacy protections for individuals regarding their individually identifiable health information.*

Generally, the following types of state laws are exempted from preemption by HIPAA:

- *State laws (including the procedures established under them) that deal with the reporting of disease, injury, child abuse, birth or death*
- *State laws that have as their principal purpose to regulate the manufacture, registration, distribution, dispensing or other control of controlled substances*
- *State laws that require health plans to report or provide access to information for purposes such as management, audits, financial audits, program monitoring and evaluation, or the licensure or certification of facilities or individuals.*

If your state has a law necessary for one of the following purposes, the Secretary of HHS has the authority to determine that the general preemption rule does not apply to that state law:

- *To prevent health care fraud and abuse*
- *For state health care reporting on delivery or costs*
- *To ensure the appropriate regulation by state authorities of insurance or health plans*
- *To serve a compelling public health, safety or welfare need (if the Secretary of HHS determines that any intrusion on privacy is warranted).*

Until the Secretary of HHS makes a determination, the HIPAA standard, requirement or implementation specification from which you are seeking an exception remains in effect. If granted, an exception remains in effect until the state law or the HIPAA standard, requirement or implementation specification is materially changed such that the grounds for the exception no longer exist or the Secretary of HHS revokes the exception based upon a determination that the grounds supporting the need for the exception no longer exist.

You must submit a request to the Secretary of HHS if your state would like to take advantage of the above-mentioned exception.

- *The request must be in writing and must be submitted by your state's chief elected official.*
- *Such requests must include the following information:*
  - ⇨ *The state law for which you are requesting an exception*
  - ⇨ *The standard, requirement or implementation specification for which you are requesting the exception*
  - ⇨ *The portion of the standard or provision that you will not implement based upon the exception or the additional data to be collected based upon the exception*
  - ⇨ *How health care providers, health plans, and other entities would be affected by approval of your request for an exception*
  - ⇨ *Reasons why the state law should not be preempted, including how your state's law meets the criteria of the exception.*

Addressing the Privacy of Health Information through State Law

Many states have health information privacy and patient access laws. Regarding health information privacy and disclosure, the states appear to have taken either (1) a comprehensive approach to protecting a wide spectrum of health information or (2) a more sector-specific approach by providing privacy protection for certain types of medical conditions, entities or situations. Many states have chosen to protect health information regarding specific medical conditions, entities or situations and also have laws dealing with patients' access rights to their health information. Due to the

number and detailed nature of these types of state statutes, we do not summarize them here. However, you can find detailed summaries of state health information laws on the Health Privacy Project's website at: http://www.healthprivacy.org/info-url_nocat2304/info-url_nocat_search.htm.

Below you will find a sampling of some of the broader approaches that have been taken to protect the privacy of patient information. Note, though, that each state should take the approach that it finds is most suitable to meet its unique needs, whether the approach is more comprehensive or sector-specific in nature. Some states also have webpages on their websites that have general HIPAA-related information. For an example of such a webpage, please see the New York Office for Technology's HIPAA webpage at: http://www.oft.state.ny.us/hipaa/index.htm.

A Note on State HIPAA Preemption: *When considering state statutory law, note that HIPAA preempts contrary provisions of state law, but does not preempt more stringent privacy provisions of state law.*

State Health Privacy Approach	State	Link to State Legal Authority	Link to Health Privacy Project
Comprehensive Statutory Access and Disclosure of Health Information: • Washington State has a comprehensive statutory structure that provides individuals with access rights to their own health information and provisions addressing when individuals' health information may be disclosed.	WA	http://www.leg.wa.gov/RCW/index.cfm?fuseaction=chapterdigest&chapter=70.02	http://www.healthprivacy.org/usr_doc/WA_2002.pdf
Comprehensive Health Information Disclosure Statutes: • Rhode Island, Florida and Wisconsin have comprehensive statutes dealing with the privacy and disclosure of health information.	RI	http://www.rilin.state.ri.us/Statutes/TITLE5/5-37.3/INDEX.HTM *(see §5-27.3)*	http://www.healthprivacy.org/usr_doc/RI_2002.pdf
	FL	http://www.flsenate.gov/statutes/index.cfm?App_mode=Display_Statute&Search_String=&URL=Ch0381/SEC026.HTM&Title=->2002->Ch0381->Section%20026 *(see §381-026)*	http://www.healthprivacy.org/usr_doc/FLORIDA2002.pdf
	WI	http://folio.legis.state.wi.us/cgi-bin/om_isapi.dll?clientID=321435322&infobase=stats.nfo&j1=146.81&jump=146.81&softpage=Browse_Frame_Pg *(see §146.81-.84)*	http://www.healthprivacy.org/usr_doc/WI2002.pdf.

Financial Information ::

Important Information Privacy Issue

An issue of importance to both the public and private sectors is protecting the privacy of personal information that is collected by financial institutions, such as banks. Of particular concern regarding financial information is what type of personal information financial institutions can collect and when and to whom they can disclose that information. Another related concern is the commission of fraudulent acts in order to obtain personal information from financial institutions.

Federal Authority on the Issue

The Gramm-Leach-Bliley-Financial Services Modernization Act of 1999 (the GLB Act), 15 USC §§6801-6810 & §§6821-6827.

- **What Does It Do?** The Gramm-Leach-Bliley Act removed legal barriers to allow for mergers between banks, insurance companies, brokerage firms and other financial entities.

  The GLB Act includes two subchapters that provide privacy protections for financial information and apply to financial institutions. The first subchapter provides protection to individuals' personal information that is collected, used and disclosed by banks and other financial institutions. Generally, financial institutions cannot disclose individuals' nonpublic personal information to a nonaffiliated third party without first providing the individual with notice of their privacy policies and the opportunity to "opt out" of such disclosures. However, the GLB Act provides exceptions under which financial institutions can disclose such information without providing a privacy policy notice or the opportunity for an individual to opt-out of the disclosure.

  The second subchapter assesses criminal penalties against those who commit fraud in an attempt to wrongfully gain access to individuals' financial information.

- **To Whom Does It Apply?** The GLB Act applies to "financial institutions." Under the GLB Act, to qualify as a "financial institution," an entity must be "significantly engaged in financial activities." Typically, banks, savings and loans, credit unions, insurance companies, securities and commodities brokerage firms, mortgage brokers, check cashers, financial advisors, and credit counselors are "financial institutions," and hence, must comply with the GLB Act's requirements. State government entities that provide financial products, such as mortgages or student loans may also be "significantly engaged in financial activities," and hence, may have to comply with the GLB Act.

- **What Elements of Control Do States Have Regarding Financial Information?** The GLB Act's financial privacy and fraudulent access provisions only preempt state financial privacy laws or regulations if they are inconsistent with the GLB Act. In such cases, a state law or regulation is only preempted to the extent of its inconsistency. Hence, states are permitted to provide financial privacy protections that are greater than those in the GLB Act as long as the Federal Trade Commission (FTC), after consultation with any other agencies with jurisdiction, determines that the greater state privacy protections are consistent with the GLB Act.

Although the GLB Act's financial privacy provisions are generally enforced by federal agencies, such as the FTC, state government insurance agencies have enforcement jurisdiction against persons domiciled in their state who provide insurance.

Link to the GLB Act's Disclosure of Personal Information Provisions:
http://www.ftc.gov/privacy/glbact/glbsub1.htm.

Link to the GLB Act's Fraudulent Access to Financial Information Provisions:
http://www.ftc.gov/privacy/glbact/glbsub2.htm.

Link to the GLB Act's Final Rule: http://www.ftc.gov/os/2000/05/65fr33645.pdf.

Application of this Privacy Issue

What Types of Financial Information are Involved in this Issue? The GLB Act provides privacy protections regarding an individual's "nonpublic personal information." Nonpublic personal information generally is any information that is personally identifying and is obtained by a financial institution in one of three ways (1) from a consumer (2) from a transaction with a consumer or from a service performed for a consumer or (3) "otherwise obtained by the financial institution." Examples of nonpublic personal information are:

- Information that a consumer provides to a financial institution on a loan, credit card or other application for a product or service
- Account balance information, payment or overdraft history or credit or debit card purchases
- The fact that an individual is or was a customer of a financial institution or obtained financial products from a financial institution
- Information disclosed in a way that indicates an individual was or is a consumer of a financial institution
- Information from a consumer that was obtained by a financial institution in connection with collecting or servicing a credit account
- Information collected through an Internet "cookie"
- Information contained in a consumer report
- Lists, descriptions or groupings of consumers that are derived by a financial institution from nonpublic personal information.

Notable types of information that are not considered to be nonpublic personal information include information that is publicly available and lists, descriptions or groupings of consumers that are derived without using nonpublic personally identifiable information. For more details about the types of information that the GLB Act protects, please consult the GLB Act's Final Rule [see §313.3 (n)-(o)].

What Types of Activities are Involved in this Issue? To qualify as a financial institution under the GLB Act, an entity must be "significantly engaged in financial activities." Examples of financial institutions that are significantly engaged in financial activities are:

- A retailer that provides credit by issuing its own credit card directly to a consumer
- A personal property or real estate appraiser
- An automobile dealership as specified in the GLB Act Final Rule
- A business that prints and sells checks to consumers
- A business that regularly wires money to or from consumers
- A check cashing business

- An accountant or tax preparation service that is in the business of completing income tax returns
- A business that operates a travel agency in connection with financial services
- An entity that provides real estate settlement services
- A mortgage broker
- An investment advisory company or credit counseling service
- A career counselor who provides services to individuals employed by or recently displaced from a financial organization or other individuals as specified in the GLB Act.

For more information about the types of activities that are within the GLB Act, please consult the GLB Act's Final Rule [see §313.3 (k)].

For those in the public sector, it is important to remember that governmental agencies and organizations that are significantly engaged in financial activities, such as providing student loans or mortgages, may be subject to the GLB Act.

Considerations for Addressing the Privacy of Financial Information

The considerations below are based upon the GLB Act's requirements that apply to financial institutions. Even if an organization or entity does not qualify as a financial institution, it may use the GLB Act's provisions as guidance on how to protect individuals' financial information.

Note that the GLB Act places requirements on financial institutions before they can disclose nonpublic personal information to entities that are not affiliated with them. However, the GLB Act does not appear to place requirements on financial institutions' disclosure of such information to their affiliated entities.

A Note on Enforcement Authority: Enforcement authority regarding the GLB Act's financial privacy provisions varies according to the type of financial institution that is regulated. For example, the Office of the Comptroller of the Currency enforces the GLB Act for national banks. The FTC regulates the enforcement of the privacy provisions of financial institutions that are not subject to the enforcement jurisdiction of another agency as specified by the GLB Act.

As a general rule, the FTC enforces the GLB Act's fraudulent access provisions, except in a few instances specified in the GLB Act.

Restrictions on Disclosures to Nonaffiliated Third Parties:

Before disclosing nonpublic personal information about an individual to a nonaffiliated third party, provide the individual with notice of your privacy practices and the opportunity to opt out, or choose not to have such information disclosed.

- *A "nonaffiliated third party" is an entity that is not an affiliate of yours. An entity that is not related to you by common ownership or that is not affiliated by corporate control also is a nonaffiliated third party of yours.*
- *Provide the individual with notice and an opportunity to opt out regardless of whether you are planning to make the disclosure directly to a nonaffiliated third party or through an affiliate of yours.*

Prior to disclosing nonpublic personal information to a nonaffiliated third party, provide an individual with the following:

- *Written or electronic notice of your privacy policies*
- *Written or electronic notice that you may disclose his or her nonpublic personal information*
- *Notice that he or she may "opt out" of such disclosures*
- *A way to "opt out" of such disclosures.*

Incorporate the following into your notice of your privacy policies and practices with respect to nonpublic personal information:

- *How you handle the disclosure of that information to affiliated third parties (including categories of disclosable information)*
- *How you handle the disclosure of that information to nonaffiliated third parties (including categories of disclosable information)*
- *How you handle the disclosure of former customers' nonpublic personal information*
- *How you protect the nonpublic personal information of consumers*
- *Categories of nonaffiliated persons to whom such information is or may be disclosed*
- *Categories of nonpublic personal information you collect*
- *How you protect the information's security and confidentiality*
- *Any disclosures required by the Fair Credit Reporting Act where the consumer has a right to opt out.*

Notice Requirements for Consumer and Customer Relationships:

The GLB Act requires financial institutions to provide privacy notices to their customers and consumers. When and how often a financial institution must provide such notices depends upon whether a notice is going to the financial institution's customer or consumer.

- *A **consumer** is someone who obtains financial services or products from a financial institution primarily for personal, family or household purposes, but with whom the financial institution does not have a continuing relationship. Examples of consumer relationships are when a person obtains an isolated financial transaction from a financial institution, such as an ATM withdrawal or one-time personal or real property appraisal services.*
- *A **customer** is someone with whom a financial institution has a continuing relationship. Like a consumer, a customer receives financial services or products primarily for personal, family or household purposes. A customer may have a credit account with or be obtaining a loan or insurance products from a financial institution.*

If you are dealing with a consumer, provide notice of your privacy policies and practices prior to disclosing the consumer's information to a nonaffiliated third party.

If you are dealing with a customer, provide notice of your privacy policies and practices when you first establish a customer relationship with him or her and not less than annually thereafter for as long as the customer relationship continues.

Exceptions to the Opt-Out Requirements:

Instances in which you may forego providing individuals with the option to opt out of disclosures of their nonpublic personal information to a nonaffiliated third party include:

- *When the nonaffiliated third party performs functions or services for you (including marketing your products or services), or*
- *Where the nonaffiliated third party has a joint marketing agreement with you.*

If you can make a disclosure under the above-described exceptions:

- *Provide the individual with notice of the disclosure, and*
- *Enter into an agreement with the nonaffiliated third party to ensure that the confidentiality of the information is maintained.*

Exceptions to Both the Notice and Opt Out Requirements:

Instances in which you may forego providing individuals with a notice of your privacy policies and an opportunity to opt out before disclosing their nonpublic personal information to nonaffiliated third parties include:

- *Where the disclosure is necessary to administer a transaction requested or authorized by the consumer*
- *Where the disclosure is necessary to administer transactions in connection with servicing a consumer's account, servicing or processing a service or product requested or authorized by the consumer, or a securitization or secondary market sale*
- *Where the consumer grants his or her consent*
- *To protect the confidentiality or security of consumer records or to prevent fraud*
- *To law enforcement agencies, the FTC, or state insurance authorities where such is permitted or required by law and is in accordance with the Right to Financial Privacy Act of 1978*
- *Where the disclosure is to a credit reporting agency in accordance with the Fair Credit Reporting Act*
- *To comply with federal, state or local legal requirements or investigations.*

Limitations on the Redisclosure of Information:

Nonaffiliated third parties can redisclose the nonpublic personal information you provide to them to:

- *Their own affiliates, or*
- *Your affiliates.*

A nonaffiliated third party also may redisclose nonpublic personal information to an entity that is not affiliated with it and also not affiliated with the financial institution from which it received the information in the following instances:

- *Where the financial institution did not have to provide privacy or opt-out notices under a GLB Act exception when it initially disclosed the information. In this case, the nonaffiliated third party can only redisclose the information to carry out that exception within the ordinary course of business.*
- *Where the financial institution disclosed the information outside of one of the GLB Act's exceptions (for example, where a consumer or customer failed to exercise his or her opt-out rights). In this case, the nonaffiliated third party can redisclose the information to its affiliates, to the financial institution's affiliates, or to anyone else to whom the financial institution could disclose it.*

Restrictions on the Sharing of Account Numbers:

Do not share consumer account numbers with nonaffiliated third parties for use in:

- *Telemarketing*
- *Direct mail marketing, or*
- *Email marketing.*

An exception to this prohibition is the disclosure of consumer account numbers to consumer reporting agencies.

A Note on the GLB Act's Fraudulent Access to Financial Information Provisions:

The GLB Act criminalizes obtaining the customer information of a financial institution under false pretenses.

- *Note that "customer" under this part of the GLB Act means a person to whom a financial institution provides a product or service, including instances in which the financial institution acts as a fiduciary.*
- *It is also illegal for one person to request that another person obtain customer information, knowing that person will have to use fraudulent means to obtain the information.*

Violations of these provisions can carry jail time and criminal fines. Generally, the FTC has administrative enforcement responsibilities for these GLB Act provisions.

The GLB Act specifies certain instances where conducting any of the above-described activities does not constitute a crime. Such instances include:

- Law enforcement agencies' obtaining of customer information from a financial institution in connection with performing their official duties
- A financial institution's obtaining of such information to test security procedures for maintaining the confidentiality of information, to investigate alleged employee misconduct or negligence or to recover customer information that was illegally obtained in violation of the GLB Act's provisions
- An insurance institution's obtaining of such information for the investigation of insurance fraud where the investigation is legally authorized by the state
- A person's obtaining of a financial institution's customer information that is available as a public record filed pursuant to securities laws
- A state-licensed private investigator's obtaining of such information to the extent reasonably necessary to collect delinquent child support."

Addressing the Privacy of Financial Information through State Law

The GLB Act provides a minimum floor of privacy protection for customers and consumers who transact business with financial institutions. However, state laws on financial privacy are not altered by the GLB Act to the extent that they are not inconsistent with the GLB Act's provisions. Hence, states may enact financial privacy laws as long as the FTC deems them to be consistent with the GLB Act.

Note, though, that the GLB Act only addresses the privacy of financial information that may be disclosed by a financial institution to nonaffiliated third parties. ***The Fair Credit Reporting Act, as recently amended, addresses the disclosure of financial and other personal information to affiliates and contains provisions that would preempt state laws regulating the sharing of such information with affiliates.***

In the first section of the table below, you will find an example of a state that has enacted financial privacy protections. It has taken an "opt-in" approach to the disclosure of individuals' financial information, meaning that the disclosure of such information is prohibited, unless the individual authorizes it. In contrast, the GLB Act takes an "opt-out" approach, which means that such information may be disclosed in the instances specified in the GLB Act, unless an individual requests that the information not be disclosed.

A Note on North Dakota: In June 2002, over 70% of North Dakotans voted in favor of requiring consent before financial institutions can disclose individuals' personal information to third parties. This was the first time such a vote was held by a state to set financial privacy protections greater than the Gramm-Leach-Bliley Act.

Financial Privacy Issue	State	Link to State Legal Authority
Taking an opt-in approach to financial information disclosures: • **Connecticut:** Connecticut takes an opt-in approach by prohibiting financial institutions from disclosing customer financial records unless authorized by the customer or in response to certain instances specified in the statute. Connecticut's financial disclosure prohibition also provides for the disclosure of a customer's financial records to certain legal authorities and has sixteen enumerated exceptions, including disclosures made to a broker-dealer or investment advisor engaged in a contractual networking arrangement with the financial institution, as long as the customer is given notice of this and an opportunity to opt-out of such disclosures.	CT	http://www.cga.state.ct.us/2003/pub/Chap664a.htm#Sec36a-42.htm *(see §36a-42 et seq.)*
Disposing of financial and other information: • Wisconsin addresses the disposal of financial and other records containing personal information. Financial institutions and medical and tax preparation businesses are restricted in their ability to dispose of personally identifiable information by state law. They must take certain measures before disposal, such as shredding records with personal information or modifying such records to make the personal information unreadable. Violations may result in civil liability to the injured party, $1000 in fines and/or a potential 90 day term of imprisonment.	WI	http://www.legis.state.wi.us/statutes/Stat0895.pdf *(see §895.505)*

Financial Privacy Issue	State	Link to State Legal Authority
Being apprised of new state confidentiality requirements: • Washington State Executive Order 00-03 provides that state agencies take steps to ensure that the appropriate personnel are aware of new state confidentiality requirements for information such as credit and debit card numbers, electronic check numbers, card expiration dates, and other financial account numbers connected with the electronic transfer of funds.	WA	http://www.governor.wa.gov/eo/eo_00-03.htm.

A Note to the Reader: This section addresses the sharing of financial information by financial institutions to nonaffiliated third parties and is based upon the requirements of the Gramm-Leach-Bliley Act. For information on the sharing of financial and other personal information among **affiliated third parties**, please consult the Fair Credit Reporting Act, 15 USC §§ 1681-1681u, as recently amended by HR2622, "The Fair and Accurate Credit Transactions Act of 2003." ***The Fair Credit Reporting Act contains provisions that address the sharing of financial and other personal information among affiliated organizations and that preempt state laws that would regulate the sharing of such information among affiliated organizations.***

Students' Education Information ::

Important Information Privacy Issue

An issue of importance especially for educational institutions and agencies is protecting the privacy of personal information contained in students' education records. The collection of students' personal information has raised questions regarding when and to whom educational institutions and agencies may disclose students' personal information.

Federal Authority on the Issue

The Family Educational Rights and Privacy Act of 1974 (FERPA), 20 USC §1232g.

- **What Does It Do?** FERPA provides privacy protection for students' education records, while ensuring a parent's right to access his or her child's education records, correct mistakes in those records, and know who has requested or obtained the records. FERPA includes exceptions to its disclosure restrictions that allow education records to be divulged to school officials or for specific law enforcement, judicial or administrative purposes. Third parties who receive education records under FERPA cannot disclose them to anyone else unless a parent consents in writing.

The U.S. Department of Education promulgated a FERPA Final Rule, which provides additional detail to FERPA's requirements. Due to the detailed nature of the FERPA statute, this publication draws upon the FERPA statute unless otherwise noted. For additional details, you may consult the FERPA Final Rule.

- **To Whom Does It Apply?** FERPA's provisions apply to any public or private agency or institution that receives funds under any of the U.S. Department of Education or Secretary of Education's applicable programs. However, FERPA's provisions on a parent's right of access to his or her child's records apply specifically to state educational agencies, regardless of whether they would otherwise come within FERPA's purview.

- **What Elements of Control Do States Have Regarding Students' Education Information?** While FERPA does not expressly permit states to enact laws that are consistent with its purpose, it does appear, for practical purposes, that states may enact laws that provide additional protections to education records as long as such laws do not conflict with FERPA. In the event an educational entity cannot comply with FERPA due to a conflict of state or local law, then, according to the FERPA Final Rule, the educational entity must notify the Family Policy Compliance Office of the U.S. Department of Education within 45 days of the conflicting law, including its text and a citation to it.

Link to FERPA: http://www4.law.cornell.edu/uscode/20/1232g.html.

Link to the FERPA Final Rule: http://www.ed.gov/offices/OII/fpco/pdf/ferparegs.pdf.

Application of this Privacy Issue

What Types of Students' Information are Involved in this Issue? Students' education records covered by FERPA are those records that contain information directly related to a student and are maintained by an educational agency or institution or a person acting for such an agency or institution. If you maintain these types of records, you may consider determining whether you are an educational agency or institution that must comply with FERPA.

However, the following types of records are specifically exempted from FERPA:

- Records of educational personnel (such as teachers' records) and administrative personnel which are in the sole possession of such personnel and are not accessible or revealed to anyone else but a substitute
- Records maintained by an educational agency or institution's law enforcement unit that were created by that unit for law enforcement purposes
- Records of an educational agency or institution's employees as long as such employees are not attending the agency or institution and the records were made in the normal course of business and are not available for use for any other purpose
- Medical records (including psychiatric records) of students 18 years of age or older or of students attending a post-secondary institution that were made during treatment and are not accessible to anyone other than those individuals treating the student.

What Types of Activities are Involved in this Issue? If you maintain the types of records described above as being within FERPA's purview, FERPA provides requirements for:

- When and how you can allow a parent to access his or her child's records
- When and how you can allow a parent to correct his or her child's records
- When and how a parent must consent before allowing a third party to access a student's records
- Who else can access student records without parental consent
- When and how specific types of student records, such as a student's information for a student directory or records on disciplinary incidences, may be disclosed.

Considerations for Addressing the Privacy of Students' Educational Information

The considerations below are based upon the requirements of FERPA. Educational agencies and institutions, as defined by FERPA, must follow those requirements. However, entities not within FERPA's purview may use FERPA's requirements for guidance in protecting the personal information of students as they deem appropriate.

A Note on the Transfer of Rights Under FERPA:

When you are dealing with the right to access, correct and consent to the disclosure of a child's education records, remember that such rights are transferred to the child upon reaching age 18 or attending a postsecondary institution. This means that, after a child reaches 18 or begins attending a postsecondary institution, only the child, not the parent, has rights and can grant permission or consent under FERPA.

Ensuring a Parent's Right of Access:

Establish procedures to permit parents to inspect and review their children's education records within a reasonable time.

- *Under FERPA, a "reasonable time" is to be no longer than 45 days after the request is made.*
- *If an educational agency or institution has a policy which denies or effectively prevents a parent's inspection and review rights, it will not receive funds under any applicable program of the U.S. Department of Education.*
- *State educational agencies and institutions must provide parents with the right to inspect and review their children's education records. If a state educational agency or institution has a policy of denying or effectively preventing such, it will not receive funds under any of the U.S. Department of Education's applicable programs. More specifically, this*

requirement applies to the records of a state educational agency or institution that are maintained on children who are or have been in attendance at any school of an educational agency or institution that is subject to FERPA.

If materials or documents in the education records of a student include information about more than one student, you may allow the parent to view only the materials or documents relating to his or her child or to be informed of the specific information contained in such part of any materials.

The following types of records are exempted from being accessed by a student at a postsecondary educational institution:

- *Parents' financial records or information*
- *Confidential letters and statements of recommendation, if placed in the student's file prior to January 1, 1975 and not used for any purpose other than those for which they were intended.*

Provide an opportunity for a parent to correct or delete any incorrect, inaccurate, misleading or otherwise inappropriate data from his or her child's records and insert an explanation as to the content of the record.

- *Educational agencies and institutions may be denied funds under the U.S. Department of Education's applicable programs for failing to provide parents with this right.*

If a parent challenges the contents of his or her child's records, provide an opportunity for a hearing in order to ensure that information in the child's records is not misleading, inaccurate or otherwise in violation of the child's privacy rights.

- *An educational agency or institution can be denied funds for failing to provide such a hearing.*

Make sure that when a student or person applying for admission to an educational institution waives his or her access rights with respect to confidential recommendations, the following requirements have been satisfied:

- *Upon the student's request, you provide the student with the names of all persons making confidential recommendations*
- *The recommendations are used solely for their intended purpose*
- *The waiver is not required as a condition to admission to school or to the receipt of financial aid or other services or benefits.*

Ensuring Parents' Right to Consent to Disclosure:

Make sure that you have a parent's written consent prior to releasing a student's education records or any personally identifiable information contained therein.

- *Educational agencies and institutions may be denied funds under any applicable program of the U.S Department of Education for having a policy or practice of releasing this type of information without a parent's consent.*

Instances in which you may release without parental consent education records or the personally identifiable information therein to other school officials include:

- *To teachers and other officials of a student's school who have a legitimate educational interest, including the student's educational interest*
- *To representatives of certain federal officials including the U.S. Comptroller General, the Secretary of Education, and Attorney General*

- *To state educational authorities for auditing purposes of federally-supported education programs.*

Instances in which you may without parental consent release education records or personally identifiable information contained therein for administrative purposes include:

- *In connection with the application for or receipt of financial aid*
- *For school studies for predictive tests, student aid or improving instruction*
- *For accrediting functions of accrediting organizations.*

Instances in which you may release without parental consent education records or personally identifiable information therein for law enforcement or judicial purposes include:

- *When ordered by a subpoena for law enforcement purposes or in connection with a federal grand jury*
- *To state and local officials under a state statute allowing disclosures concerning the juvenile justice system in order to better serve juveniles (where such a statute was enacted after November 19, 1974, officials receiving such disclosures must certify in writing that they will not further disclose the information without a parent's consent unless otherwise permitted by state law).*

You may also release a child's education records without parental consent in emergency situations, when such is necessary for the student's or another person's health or safety.

- *This provision is subject to the regulations of the Secretary of Education.*

You may release the education records or personally identifiable information of a dependent child to the parents.

When asked to transfer records because a child wishes to enroll in another school, you must take the following steps under FERPA:

- *Notify the parents of the transfer of the records to the other school*
- *Provide the parents with a copy of the records, if they request them*
- *Provide the parents an opportunity for a hearing if they challenge the contents of the records.*

When you transfer a student's personal information to a third party, the third party cannot permit anyone else to access the records without a parent's consent.

- *If a third party outside of the educational agency or institution violates this restriction or fails to destroy the information after its use in a study, the agency or institution must not allow that third party access to any education records for a minimum of 5 years.*

Make sure that you keep a record of who has requested or obtained access to a child's education records.

- *You must indicate the legitimate interest of persons who have accessed a child's records.*
- *You must make sure that only parents, school officials who are custodians of such records, other school officials with a legitimate educational interest, or others in connection with the auditing of the operations of such a system have access to these records.*

Informing Parents of Their Rights:

Inform parents of their rights with respect to their children's education records.

- *An educational agency or institution can be denied funds under the U.S. Department of*

Education's applicable programs for failing to inform parents of their rights under FERPA.
- *If a student is 18 or attending a postsecondary educational institution, the student, not the parent, must be informed of his or her rights under FERPA.*

Handling Students' Directory Information:

You may make a student's "directory information" publicly accessible as long as you fulfill the following requirements:

- *You have given public notice of the categories of information that may be made public*
- *You have allowed parents a reasonable time period after notice in which to inform you that they would like for you to obtain their consent before releasing any such directory information.*

Directory information includes the following information about a student:

- *Name*
- *Address*
- *Phone number*
- *Date and place of birth*
- *Major*
- *Participation in school activities or sports*
- *Weight and height for members of athletic teams*
- *Dates of attendance*
- *Degrees received*
- *Awards received*
- *Most recent educational institution previously attended.*

Handling Disciplinary and Other Records:

You may include information in an educational record about disciplinary actions taken after a student displayed conduct that posed a significant risk to the safety or well-being of that student, other students, or other members of the school community.

You may disclose such disciplinary information to teachers and school officials who have a legitimate educational interest in the child's behavior.

You also may disclose such information to a teacher or school officials of other schools where they have a legitimate educational interest in the child's behavior.

If you are an institution of higher education, you may disclose to a parent or legal guardian, information about a student's violation of a federal, state or local law or any rule or policy of the educational institution governing the use or possession of alcohol or a controlled substance as long as the child is under 21 and the institution has determined that the student committed a disciplinary violation with respect to such use or possession. Note that you may make this disclosure regardless of whether the information is actually contained in the student's education records.

Addressing the Privacy of Education Records through State Law

Since FERPA sets a federal minimum on privacy for students' education records, a state may refer to FERPA in its own statutes. For example, a Utah state statute regarding the privacy of education records specifies that "[e]mployees and agents of the state's public education system

shall protect the privacy of students, their parents, and their families, and support parental involvement in the education of their children through compliance with the protections provided for family and student privacy under Section 53A-13-302 and the Federal Family Educational Rights and Privacy Act…." Louisiana also has a similar statute that states that "[a]n education record of a student may be inspected by the student or his or her parents in accordance with the federal Family Educational Rights and Privacy Act."

- Link to the Utah statute (see §53A-13-301): http://www.le.state.ut.us/~code/TITLE53A/htm/53A0E023.htm.
- Link to the Louisiana statute [see §17:112 (D)]: http://www.legis.state.la.us/tsrs/tsrs.asp?lawbody=RS&title=17&section=112.

Like Utah, some states also have put in place additional protections through state laws, regulations or policies. Below you will find additional examples of state protections for student records.

Education Privacy Issue	State	Link to State Legal Authority
Providing for a general right of student record confidentiality: • Wisconsin provides for a general right of confidentiality for student records, with certain exceptions, which are noted in the applicable Wisconsin statute. Wisconsin also provides the school board with the authority to adopt regulations to maintain the confidentiality of student records.	WI	http://www.legis.state.wi.us/statutes/Stat0118.pdf *(see §118.125(2))*
Addressing specific types of student records: • Wisconsin has a statute that defines and contains provisions dealing with specific types of student records, including "behavior records," "progress records," and "pupil physical health records."	WI	http://www.legis.state.wi.us/statutes/Stat0118.pdf *(see §118.125)*
Right of a child to deny a parent or legal guardian's access to his or her private or confidential information: • Under Minnesota law, a child may request that an authority withhold his or her private or confidential information from his or her parent or legal guardian. The authority responsible for providing access to the child's private or confidential information may grant the child's request if such is in the best interest of the child. By rule, this right does not extend to private educational data and records (Minnesota Rules §1205.0500)	MN	http://www.revisor.leg.state.mn.us/stats/13/02.html *(see §13.02 (8))* http://www.revisor.leg.state.mn.us/arule/1205/0500.html
Prohibition on withholding education records because of an outstanding obligation: • Louisiana prohibits withholding a student's records because of an outstanding fine, debt or other obligation.	LA	http://www.legis.state.la.us/tsrs/tsrs.asp?lawbody=RS&title=17&section=112 *(see §17:112 (C))*

Social Security Numbers ::

Important Information Privacy Issue

An issue of importance is protecting the privacy of Social Security Numbers (SSNs). According to a May 2002 U.S. General Accounting Office report on SSNs, the SSN was created by the federal government in 1936 as an identifier of individuals for purposes of tracking workers' earnings and their eligibility for Social Security benefits. However, SSNs are currently used by state and local governments and the commercial sector. The use of SSNs as identifiers has raised concerns about the facilitation of identity theft through the unauthorized use of individuals' SSNs. Hence, those entities that collect, use or disclose individuals' SSNs must be careful to protect against their falling into the wrong hands.

Federal Authority on the Issue

The Privacy Act of 1974 (the Privacy Act), 5 USC §552a (see also Public Law 93-579 §7).

- **What Does It Do?** Section 7 of the Privacy Act prohibits all levels of government from denying an individual a right, privilege or benefit because that individual refuses to disclose his or her SSN. However, the Privacy Act provides for exceptions in certain instances. Government agencies that collect an individual's SSN must inform that individual of whether the disclosure is mandatory or voluntary, the statutory authority under which the agency is requesting the SSN, and how the SSN will be used.

- **To Whom Does It Apply?** The Privacy Act's provisions as they relate to SSNs apply to federal, state and local governments.

- **What Elements of Control Do States Have Regarding SSNs?** The Privacy Act provides for several exceptions to its general prohibition on the denial of a right, benefit or privilege based upon an individual's refusal to disclose his or her SSN. These exceptions are detailed later in this section.

- **A Note on other Provisions of the Privacy Act:** The Privacy Act is a broad statute that, in addition to SSNs, protects against federal agencies' unauthorized use and disclosure of records that identify an individual and relate to such areas as education, financial transactions, medical history and criminal or employment history. The Privacy Act contains twelve enumerated exceptions to allow for the disclosure of such information. Other Privacy Act provisions seek to protect the integrity of federal government information by allowing individuals to access and amend, if incorrect, their personal information.

Since these provisions apply to federal agencies, this section does not address those provisions of the Privacy Act. However, states and others may consider examining those provisions of the Privacy Act when determining how to protect individuals' personal information.

Link to the Privacy Act: http://www4.law.cornell.edu/uscode/5/552a.html.

Link to the Privacy Act's Provisions on SSNs (see Note on "Disclosure of Social Security Number"): http://www4.law.cornell.edu/uscode/5/552a.notes.html.

NOTE: *Section 7 of the Privacy Act was not codified in the United States Code.*

Link to U.S. Department of Justice Information on the Protection of SSNs Under the Privacy Act: http://www.usdoj.gov/04foia/1974ssnu.htm.

Link to U.S. General Accounting Office (GAO) Report on SSN Use, GAO-02-352 (May 2002): http://www.gao.gov/new.items/d02352.pdf.

Link to U.S. Social Security Act Authorization of State Use of Social Security Numbers, 42 USC §405 (c)(2)(C)(i): http://www4.law.cornell.edu/uscode/42/405.html.

Application of this Privacy Issue

What Types of Information are Involved in this Issue? The Privacy Act specifically applies to SSNs collected by federal, state and local government agencies.

What Types of Activities are Involved in this Issue? Federal, state and local government agencies must adhere to the Privacy Act's requirements when they collect SSNs.

Considerations for Addressing the Privacy of SSNs

Since the Privacy Act regulates federal, state and local governments' handling of SSNs, some of the considerations below are mandated by the Privacy Act. Where this is the case, it is noted.

If you, as a federal, state or local government agency, collect SSNs from individuals, the Privacy Act prohibits you from denying an individual a right, privilege or benefit because the individual refuses to disclose to you his or her SSN.

Under the following exceptions provided for in the Privacy Act, you may refuse an individual a right, privilege or benefit if he or she refuses to disclose a SSN:

- *If the disclosure is mandated by a federal statute*
- *If your agency's system of records was in existence and operating before January 1, 1975, as long as SSN disclosures were required under a statute or regulation adopted prior to that date in order to verify an individual's identity*
- *If the disclosure is made when you are using SSNs in administering taxes, public assistance or driver's license or motor vehicle registration laws [this exception can be found in the Tax Reform Act of 1976, 42 USC §405(c)(2)(C)(i), (iv) (2000)].*

Under the Privacy Act, when you collect an individual's SSN, you must inform the individual of the following:

- *Whether the collection of SSNs is voluntary or mandatory*
- *The statutory authority under which you are collecting SSNs, and*
- *How you will use the individual's SSNs.*

Addressing the Privacy of SSNs through State Law

Some states have enacted legislation regarding the disclosure and use of SSNs. Below are examples of the approaches a few states have taken through the enactment of legislation to prevent SSNs from being disclosed to those who may use them for fraudulent or unlawful purposes. While states can take an approach to protecting SSNs through a broad statute, as

Minnesota has, states may also choose to address the protection of SSNs on a more sector-specific basis, such as protecting SSNs on specific government documents.

SSN Privacy Issue	State	Link to State Legal Authority
Classifying SSNs as private data to protect them from public disclosure: • Minnesota has taken this approach regarding SSNs collected or maintained by a state agency, statewide system or political subdivision. The only exception to access to individuals' SSNs is when such access is specifically authorized by law. However, an individual has the right to access his or her own SSN.	MN	http://www.revisor.leg.state.mn.us/stats/13/49.html *(see §13.355 & §13.02)* http://www.revisor.leg.state.mn.us/stats/13/ *(see Chapter 13's access to government data provisions)*
Protecting personally identifiable information generally and protecting SSNs from release via open records laws in specific instances: • Wisconsin has taken this approach. SSNs are exempted from disclosure in cases, such as employee pensions, tax returns and recreational licenses.	WI	http://www.legis.state.wi.us/statutes/Stat0040.pdf *(see §40.07(1) on employee trust fund privacy)* http://www.legis.state.wi.us/statutes/Stat0071.pdf *(see §71.78(1) on tax return privacy)* http://www.legis.state.wi.us/statutes/Stat0029.pdf *(see §29.024(2r)(c) on natural resources licensee privacy)* http://www.legis.state.wi.us/statutes/Stat0101.pdf *(see §101.02(21)(b) on commerce licensee privacy)* http://www.legis.state.wi.us/statutes/Stat0118.pdf *(see §118.19(1m)(a) on teacher licenses and certification privacy)*
Providing individuals with the option to restrict the release of SSNs and other personal identifiers in lists of more than 10 persons: • Wisconsin requires that agencies issuing lists of more than 10 persons with personal identifiers provide individuals the right to opt-out of such lists. This includes Wisconsin agencies, such as the Departments of Motor Vehicles, Natural Resources and Regulation and Licensing.	WI	http://www.legis.state.wi.us/statutes/Stat0085.pdf *(see §85.103 for the Department of Motor Vehicles' statute)* http://www.legis.state.wi.us/statutes/Stat0023.pdf *(see §23.45 for the Department of Natural Resources' statute)* http://www.legis.state.wi.us/statutes/Stat0440.pdf *(see §440.14 for the Department of Regulation and Licensing's statute)*

SSN Privacy Issue	State	Link to State Legal Authority
Providing requirements for notice when personally identifiable information, including SSNs, is shared between agencies: • Wisconsin requires that, when agencies wish to exchange personally identifiable information with each other, they file a notice with the Public Records Board.	WI	http://www.legis.state.wi.us/statutes/Stat0019.pdf *(see §19.69 on computer matching)*
Restricting the use of personal identifiers, such as SSNs, by institutions of higher education: • Washington State restricts institutions of higher education from using the SSNs of students, faculty and staff for identification, except for certain statutorily-specified purposes, such as for employment, financial aid, research, assessment, accountability or transcript purposes or as required by state or federal law. Washington State also requires that institutions of higher education develop a system of student personal identifiers for grading and other administrative purposes but prohibits institutions of higher education from using SSNs as personal identifiers. Wisconsin also requires that unique identifiers other than SSNs be assigned to students and used unless otherwise required.	WA	http://www.leg.wa.gov/RCW/index.cfm?fuseaction=section&section=28B.10.042 *(see §28B.10.042)* http://www.legis.state.wi.us/statutes/Stat0036.pdf *(see §36.11(35) for universities and SSNs)* http://www.legis.state.wi.us/statutes/Stat0038.pdf *(see §38.14(14) for the state technical college system and SSNs)*
Requiring that SSNs and driver license numbers may not be part of a professional license: • Washington State has taken this approach. It also has a statute that specifies that licenses containing such information that are already in existence on January 1, 2002, should comply with the statute by the next renewal date.	WA	http://www.leg.wa.gov/RCW/index.cfm?fuseaction=section&section=43.24.084 *(see §43.24.084)*
Allowing the collection of SSNs from applicants for specified licenses in order to assist in child support enforcement as required by federal law: • Washington State has a statute that requires the collection of SSNs in order to assist in the collection of child support as required by federal law. It requires that all applicants submit a SSN for an original, replacement or renewal of a professional license, commercial driver's license, occupational license or recreational license. The statute specifies that the SSN must be recorded on the license application but not on the license document itself. Note that the statute does not require the collection of SSNs for noncommercial driver's licenses prior to the time necessary to comply with the federal deadline. State licensing agencies are prohibited from disclosing the SSNs collected under this provision except as required by state or federal law.	WA	http://www.leg.wa.gov/RCW/index.cfm?fuseaction=section&section=26.23.150 *(see §26.23.150)*

SSN Privacy Issue	State	Link to State Legal Authority
Restricting the recording upon a check during a retail sale of the purchaser's SSN as a means of identification: • Rhode Island has taken this approach. Rhode Island's statute also prohibits the recording of a purchaser's credit card number upon a check as means of identification with an exception of allowing requests for the production or the recording of a credit card number as a condition for cashing or accepting a check under certain circumstances specified in the statute. Similarly, Wisconsin restricts the recording of personally identifiable information in credit card transactions as well as restricting the recording of credit card information for check cashing.	RI WI	http://www.rilin.state.ri.us/statutes/title6/6%2D13/6%2D13%2D15.htm *(see §6-13-15)* http://www.legis.state.wi.us/statutes/Stat0423.pdf *(see §423.401 for credit card transactions and §423.402 for check transactions)*
Enacting legislation and issuing recommendations regarding the confidentiality of SSNs held by individuals and non-governmental entities: • California has developed recommendations on SSNs, which include a discussion of the state's SSN statutes.	CA	http://www.privacyprotection.ca.gov/ssn/ssn.htm

Homeland Security-Related Information ::

Important Information Privacy Issue

An issue of importance to all levels of government is protecting the privacy of citizens' information while serving the interest of homeland security in preventing acts of domestic terrorism. With increased surveillance activities, information sharing, and a heightened emphasis on identifying individuals for various security-related purposes, the government also faces heightened concerns about the protection and use of citizens' personal information.

Federal Authority on the Issue

The United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (the USA Patriot Act), Public Law 107-56.

- **What Does It Do?** The USA Patriot Act, enacted by Congress in response to the September 11, 2001 terrorist attacks, provides for enhanced law enforcement investigatory tools and aims to deter and punish acts of terrorism domestically and worldwide. Its major provisions deal with the following:
    - Enhancing domestic security against terrorism
    - Enhancing surveillance procedures
    - International money laundering abatement & anti-terrorism financing
    - Protecting the border
    - Removing obstacles to investigating terrorism
    - Providing for victim relief
    - Increasing information sharing for critical infrastructure protection
    - Strengthening criminal laws against terrorism
    - Improving intelligence.

  The USA Patriot Act also makes amendments to such privacy laws as the Family Educational Rights and Privacy Act (FERPA, which addresses student privacy) and the Fair Credit Reporting Act (FCRA, which addresses credit information privacy). Those changes are detailed below.

  This section also discusses amendments made by the USA Patriot Act to technology-related laws, such as:
    - The Electronic Communications Privacy Act of 1986 (ECPA)
    - The Computer Fraud and Abuse Act of 1984 (CFAA)

- **To Whom Does It Apply?** Since the USA Patriot Act amends the provisions of a number of previously existing laws, the answer to this question is addressed, to a large extent, by whether the underlying laws that were amended by the USA Patriot Act apply to state government.

- **What Elements of Control Do States Have Regarding Homeland Security Information?** The USA Patriot Act provides additional surveillance powers to the government, including state and local law enforcement, as well as providing for additional remedies for computer-related violations.

Link to the USA Patriot Act: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_bills&docid=f:h3162enr.txt.pdf.

Other Federal Laws of Homeland Security Interest ::

Below is background on two federal laws that have a bearing on technology and privacy and that were amended by the USA Patriot Act.

The Electronic Communications Privacy Act of 1986:

The Electronic Communications Privacy Act of 1986 (ECPA) can be found at 18 USC §2510-2522 (federal wiretap statute), §2701-2711 (stored electronic and communications access), §3121 (pen register and trap and trace devices), and §1367 (interference with satellite transmissions).

- **What Does It Do?** ECPA amended the federal wiretap statute to provide protection against the unauthorized interception of specific types of electronic communications, such as email, radio-paging devices, cell phones, private communications carriers, and computer transmissions. Prior to ECPA's enactment, only wire and oral communications were legally protected against unauthorized interceptions.

  Of particular importance to state government is a set of ECPA's provisions that regulate who has access to the stored wire and electronic communications of electronic communication services and remote computing services. ECPA contains provisions that address when the government can access such communications. Other provisions of ECPA also deal with the use of pen registers and trap and trace devices, and with prohibitions against intentionally or maliciously interfering with satellite transmissions.

- **To Whom Does It Apply?** ECPA regulates access, including that of government, to the stored wire and electronic communications and transaction records of electronic communication service providers and remote computing services.
  - *A remote computing service is "the provision to the public of computer storage or processing services by means of an electronic communications system."*
  - *An electronic communication service is "any service which provides to users thereof the ability to send or receive wire or electronic communications."*

Links to ECPA's Provisions:

Federal Wiretap Statute (18 USC §§2510-2522):
http://www4.law.cornell.edu/uscode/18/pIch119.html.

Stored Electronic and Communications Access (18 USC §§2701-2711):
http://caselaw.lp.findlaw.com/casecode/uscodes/18/parts/i/chapters/121/toc.html.

Pen Register and Trap and Trace Devices (18 USC §3121):
http://caselaw.lp.findlaw.com/scripts/ts_search.pl?title=18&sec=3121.

Interference with Satellite Transmissions (18 USC §1367):
http://caselaw.lp.findlaw.com/scripts/ts_search.pl?title=18&sec=1367.

The Computer Fraud and Abuse Act of 1984:

The Computer Fraud and Abuse Act of 1984 (CFAA) can be found at 18 USC §1030.

- **What Does It Do?** CFAA was enacted in the advent of increased computer hacking in the 1980's and made illegal the unauthorized access to U.S. government computers. Through subsequent amendments in 1986, 1994 and 1996, CFAA was broadened to protect computers used in interstate commerce and to prohibit trafficking in computer passwords. CFAA currently makes it illegal to access certain computers, such as U.S. government computers and computers used in interstate commerce, and to access a computer without authorization to gain sensitive information, such as national defense or foreign relations information. It also prohibits the furtherance of fraud through unauthorized access to computers engaged in interstate commerce. Finally, CFAA makes it illegal to damage certain types of computers specified in the statute by accessing them without authorization or transmitting to them a program, information or code.

- **To Whom Does It Apply?** CFAA's provisions generally apply to "protected computers," which are computers used by or for financial institutions or the US government or which are used in interstate commerce or foreign communications. Because many state computers are used in interstate commerce, CFAA, as amended, may be broad enough to protect many state computer systems. Note that the USA Patriot Act amended the definition of a "protected computer" to include computers physically located outside of the U.S. that are used in a way that affects "interstate or foreign commerce or communications of the United States."

Link to CFAA: http://www4.law.cornell.edu/uscode/18/1030.html.

Application of this Privacy Issue

- **What Types of Information are Involved in this Issue?** The following types of information are regulated by ECPA's provisions:

  - **Wire communications**, which are "any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce."

  - **Electronic communications**, which means "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce." Electronic communications do not include wire or oral communications, communications made through a tone-only paging device, communications from a tracking device or electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds.

The USA Patriot Act contains provisions regarding the safeguard and disclosure of the following types of homeland security-related information:

- ⇨ **Foreign intelligence**, which is "information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities."

- ⇨ **Counterintelligence**, which is "information gathered, and activities conducted, to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities."

- ⇨ **Foreign intelligence** information, which is information (whether or not concerning a person of the United States) that relates to the ability of the U.S. to protect against the following acts of a foreign power or a foreign power's agent:
  - Actual or potential attacks or other grave hostile acts
  - Sabotage or international terrorism
  - Clandestine intelligence activities.

Foreign intelligence information also includes information (whether or not concerning a person of the United States) with respect to a foreign power or foreign territory that relates to the U.S.'s national defense, security or conducting of foreign affairs.

- **What Types of Activities are Involved in this Issue?**
  ECPA deals with the following activities involving the wire and electronic communications held by electronic communication providers and remote computing services:
  - ⇨ Who can access such communications when in storage
  - ⇨ Who can receive disclosures of the contents of such communications
  - ⇨ Who can receive disclosures of information about customers of such service providers.

  ECPA also deals with the use of pen registers and trap and trace devices, including when those devices are used on the Internet and computer networks.
  - ⇨ A **Pen Register** is "a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication, but such term does not include any device or process used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device or process used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of business."
  - ⇨ A **Trap and Trace Device** is "a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication."

The CFAA deals with the following:

- ⇨ Unauthorized access to protected computers
- ⇨ Damage to protected computers
- ⇨ Trafficking in computer passwords.

Considerations for Addressing the Privacy of Homeland Security-Related Information

This section addresses the privacy of information as it relates to homeland security efforts. Since the USA Patriot Act made important amendments to such statutes as ECPA and CFAA, this section addresses the USA Patriot Act in the context of those laws. The discussion below focuses on:

- Access to stored wire and electronic communications
- The use of pen registers and trap and trace devices under ECPA
- The hacking of computers under the CFAA.

Where the USA Patriot Act amended these laws, it is noted.

1: Stored Electronic and Wire Communications Under ECPA

Prior to the USA Patriot Act, for stored wire communications, such as voicemail messages, the federal wiretap statute required that law enforcement obtain a wiretap order for access. However, the USA Patriot Act amended ECPA to take the governance of access to stored wire communications out of the federal wiretap statute and place it under the provisions governing access to stored electronic communications (18 USC §2701-11). The net effect of this amendment is that the government must only obtain a search warrant to gain access to stored wire communications, a less burdensome task than obtaining a wiretap order. ***This amendment is subject to the USA Patriot Act's sunset provision.***

Access to Stored Wire and Electronic Communications:

It is illegal for anyone to intentionally access, without authorization, the facility of an electronic communication service and obtain, alter or prevent access to wire or electronic communications that are stored in the facility.

ECPA violations can result in a penalty of imprisonment for not more than one year or a fine or both. For subsequent ECPA convictions, the penalty increases to not more than five years in prison or a fine or both.

For offenses committed under the following circumstances, the penalty increases to a prison sentence for not more than five years or a fine or both:

- *To gain a commercial advantage*
- *To cause malicious destruction or damage*
- *For private commercial gain*

A Note on Sunset Provisions and the USA Patriot Act:

Some of the USA Patriot Act's provisions sunset or expire on December 31, 2005. Where a provision of the USA Patriot Act will sunset, such is noted. One notable exception is that the USA Patriot Act's provisions do not expire with respect to any foreign intelligence investigation that began before the date on which the provisions expired under the sunset provision or with respect to an offense or potential offense that began or occurred before the date on which the provisions expired.

- *In futherance of any criminal or tortious act in violation of federal or state law.*

Exceptions to the prohibition on access to stored wire or electronic communications include:

- *Where the provider of a communications service authorizes access*
- *Where the user of a communications service authorizes access to or from that user*
- *Where a governmental entity is authorized to access such information under other legal provisions.*

Note that the "Cyber Security Enhancement Act of 2002," §225 of Public Law 107-296, increased penalties for ECPA violations as reflected above.

Disclosure of the Contents of Stored Wire or Electronic Communications:

Electronic communication service providers and remote computing services generally cannot knowingly disclose the contents of the communications that they store, maintain or carry. Exceptions include disclosures to:

- *The addressee or intended recipient of the communication*
- *With the consent of the communication's originator, addressee or intended recipient or the subscriber of a remote computing service or*
- *To a law enforcement agency where the provider inadvertently obtained the contents, which appears to relate to the commission of a crime.*

USA Patriot Act Amendment: The USA Patriot Act added a provision allowing providers to disclose the contents of communications where the provider in good faith believes that an emergency involving danger of death or serious physical injury to any person requires disclosure of the information without delay. ***This amendment is subject to the USA Patriot Act's sunset provision.***

Note that the "Cyber Security Enhancement Act of 2002," §225 of Public Law 107-296, clarified that the disclosure must be made to a federal, state or local authority.

For access to the contents of stored wire or electronic communications from an electronic communication service provider the following rules apply:

- *If the information has been stored by the provider for 180 days or less, a governmental entity must obtain a federal or equivalent state search warrant.*
- *If the information has been stored by the provider for more than 180 days, a governmental entity must obtain a federal or state search warrant, a court order, or an administrative, grand jury or trial subpoena.*
- *If the service provider is a remote computing service, then a governmental entity must obtain a federal or state search warrant, a court order, or an administrative, grand jury or trial subpoena.*

Notice Requirement: *The governmental entity must provide the subscriber or customer with notice of the disclosure unless access is gained pursuant to a search warrant.*

USA Patriot Act Amendment: The USA Patriot Act amended the federal wiretap statute to allow any investigative or law enforcement officer, or attorney for the government, who has obtained knowledge of the contents of any wire, oral or electronic communication or evidence derived from any such communication, to disclose that information to federal officials, such as federal law enforcement or intelligence officials. In order to make a disclosure, the information

must include foreign intelligence, counterintelligence or foreign intelligence information. ***This amendment is subject to the USA Patriot Act's sunset provision.***

- *An investigative or law enforcement officer includes officers who are with a state government or political subdivision thereof. Those officers must be empowered to conduct investigations or make arrests under the wiretap statute.*

Disclosure of Customer Records and Information:

USA Patriot Act Amendment: The USA Patriot Act added a provision prohibiting electronic communication services and remote computing services from knowingly divulging customer or subscriber records or other information pertaining to a customer or subscriber (not including the contents of communications) to the government. A notable exception to this rule is that a service provider may disclose such records "if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person justifies disclosure of the information." ***This amendment is subject to the USA Patriot Act's sunset provision.***

Other exceptions under which service providers are required to disclose customer records or information to the government include when the government:

- *Obtains a warrant*
- *Obtains a court order*
- *Obtains the consent of the subscriber or customer*
- *Submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud.*

No Notice Requirement: *A governmental entity is NOT required to provide notice to the customer or subscriber of the receipt of the records.*

A governmental entity can access the following types of customer or subscriber information of an electronic communication or remote computing service (as long as it has a federal or state search warrant, a court order or a federal or state administrative, grand jury or trial subpoena):

- *Name*
- *Address*
- *Local and long distance telephone billing records*
- *Phone number*
- *Length of service*
- *Type of service utilized*
- *Records of session times and duration*
- *Temporarily assigned network addresses*
- *The means and source of payment, including credit card numbers and bank accounts.*

USA Patriot Act Amendment: The USA Patriot Act expanded the types of customer or subscriber records the government can access to include the type of service utilized, session times and duration records, temporarily assigned network addresses, and the means and source of payment. ***This amendment is NOT subject to the USA Patriot Act's sunset provision.***

An electronic communication service or remote computing service also may disclose customer records and information (not including the contents of communications):

- *With the customer's consent*
- *As necessary to render services to the customer or to protect the provider's rights or property*

- *As otherwise authorized by ECPA*
- *To any other person than a governmental entity.*

Violations of ECPA:

ECPA provides for administrative disciplinary proceedings where the U.S. government or one of its agencies has violated ECPA's provisions.

USA Patriot Act Amendment: The USA Patriot Act added a provision making it an ECPA violation for an investigative or law enforcement officer to willfully disclose information held by a federal agency about an individual, where the investigative or law enforcement officer receives the information via one of ECPA's mandatory disclosure provisions or via a pen register or trap and trace device and discloses it in a way that is not within the proper performance of official duties.

ECPA provides for civil actions by those aggrieved by violations of its stored wire and electronic communication provisions. Damages may be assessed in the sum of actual damages (including any profits made by the violator as a result of committing the violation), punitive damages (if the violation is willful or intentional), and court costs and attorneys fees. The minimum amount of actual damages is $1,000. However, as amended by the USA Patriot Act, ECPA does not provide for these types of civil lawsuits against the United States government.

Amendments made to ECPA's violation provisions are subject to the USA Patriot Act's sunset provision.

2: Use of Pen Registers and Trap and Trace Devices under ECPA

The government must obtain a court order to use a pen register or trap and trace device. Exceptions apply where the provider of an electronic or wire communication service must use such devices:

- *In its operations*
- *To record the fact of a wire or electronic communication to protect itself or a user from abusive use of its service*
- *To protect its rights or property*
- *With the consent of the user.*

USA Patriot Act Amendment: The USA Patriot Act amended ECPA to allow law enforcement to use pen registers or trap and trace devices on the Internet and computer networks. It also allows court orders for such devices to have a nation-wide effect. ***This amendment is NOT subject to the USA Patriot Act's sunset provision.***

Violations may result in a fine or up to one year in jail or both.

3: Other Miscellaneous Provisions of ECPA

Other provisions of ECPA also address:

- *Disclosures by video service providers (see 18 USC §2710)*
- *Interference with satellite transmissions (see 18 USC §1367)*

4. Unauthorized Access to and Use of Computers and Passwords under CFAA

Unauthorized Access to a Computer:

For state governments and other entities that have computers that qualify as "protected computers," the following types of unauthorized access are illegal:

- *Intentionally accessing a computer without authorization and obtaining information from a protected computer, if the conduct involves interstate or foreign communications*
- *Knowingly and with the intent to defraud, accessing a protected computer without authorization and obtaining anything of value (unless what is obtained by the fraud is only the use of the computer and has a value that does not exceed $5,000 in a one-year period).*

Other types of unauthorized access violations under CFAA include:

- *Intentionally accessing without authorization a U.S. government agency or department computer*
- *Intentionally accessing a computer without authorization and obtaining financial information from a financial institution or from a U.S. government agency or department or information contained in the file of a consumer reporting agency*
- *Knowingly accessing a computer without authorization and gaining protected information, such as information regarding national defense or foreign relations, with reason to believe that the information could be used to injure the U.S. or give an advantage to a foreign nation, and communicating or attempting to communicate such information or willfully keeping the information from an officer or employee of the U.S. who is entitled to receive the information.*

Damaging a Protected Computer:

If a state government computer qualifies as a "protected computer," then the following types of conduct are illegal:

- *Knowingly transmitting a program, information, code or command and intentionally damaging a protected computer*
- *Intentionally accessing, without authorization, a protected computer and recklessly damaging it*
- *Intentionally accessing, without authorization, a protected computer and causing damage to the computer.*

For these activities to violate CFAA, they must result in one of the following:

- *Damage in the amount of $5,000 or more during a one-year period*
- *Modification or impairment (or potential modification or impairment) of medical treatment or care*
- *Physical injury*
- *A threat to public health or safety, or*
- *Damage to a government computer system used in the administration of justice, national defense or national security.*

USA Patriot Act Amendment: The USA Patriot Act includes the following clarifying amendments regarding violations that cause damage to a protected computer in the amount of $5,000 or more:

- *Violators do not have to intend to cause $5,000 worth of damage, but need only intend to impair data, program, system or information integrity or availability.*
- *Monetary losses "from a related course of conduct affecting one or more other protected computers" from a one-year period may be aggregated to meet the $5,000 loss threshold.*

USA Patriot Act Amendment: The USA Patriot Act added as an offense damaging a protected computer used by or for a governmental entity for the administration of justice or national defense or security, even if the damage that results does not exceed $5,000.

Other Types of Conduct Criminalized by CFAA:

The CFAA also criminalizes the following types of activities:

- *Knowingly trafficking in computer passwords with the intent to defraud, where interstate or foreign commerce is affected or where the computer that may be accessed is a U.S. government computer.*
- *Extorting from persons or entities, including educational institutions and government entities, something of value by sending a threat to damage a protected computer through interstate or foreign commerce.*
- *Any attempt to violate any of the CFAA's provisions.*

Criminal Penalties, Private Right of Action, and Other Remedies:

Criminal penalties for violations of CFAA generally include criminal fines and jail sentences. Repeat violations may result in increased penalties.

USA Patriot Act Amendment: The USA Patriot Act amended the CFAA to allow previous state law felonies for unauthorized access to a computer to trigger CFAA's provision that increases maximum penalties for repeat offenders. Other consequences for violators of the CFAA that are provided for by the USA Patriot Act include:

- *Use of a CFAA violation as a predicate offense for obtaining a wiretap order to intercept wire communications (**this amendment is subject to the USA Patriot Act's sunset provision**)*
- *Law enforcement's interception of communications of those who access "protected computers" without authorization (**this amendment is subject to the USA Patriot Act's sunset provision**)*
- *If a violation of CFAA qualifies as a "serious computer crime," then a CFAA violation may rise to the level of the commission of a terrorist offense.*

The Cyber Security Enhancement Act of 2002, Public Law 107-296, added a maximum penalty of life in prison for knowingly or recklessly causing or attempting to cause death by transmitting a program, code, information or command and thereby damaging a protected computer.

The CFAA allows individuals who suffer damage or loss due to a CFAA violation to seek compensatory damages and injunctive relief.

USA Patriot Act Amendment: The USA Patriot Act amended the CFAA to qualify that a civil lawsuit by an individual may only be brought against a CFAA violator if the violation involves one of the following factors:

- *Causes damage of $5,000 or more within a one-year period*
- *Results in the modification or impairment (or potential modification or impairment) of medical treatment or care*
- *Results in physical injury*

- *Causes a threat to public health or safety, or*
- *Damages a government computer system used in the administration of justice, national defense or national security.*

5: Amendments to Other Federal Privacy Laws

The USA Patriot Act amends the two federal privacy laws listed below as follows:

- ***Family Educational Rights and Privacy Act of 1974 (FERPA), 20 USC §1232g:*** *The USA Patriot Act amended this law by adding a provision requiring educational institutions to disclose a student's education records where the U.S. Attorney General obtains an ex parte order for such records to investigate and prosecute domestic or international terrorism.*
- ***Fair Credit Reporting Act of 1970 (FCRA), 15 USC §1681-§1681v:*** *The USA Patriot Act amended this law by allowing for FBI officials lower in the chain of command to require consumer reporting agencies to disclose records on consumers where the information is sought for international terrorism purposes or clandestine intelligence activities. Consumer reporting agencies also can furnish consumer reports to a government agency that is authorized to conduct investigations or intelligence or counterintelligence related to international terrorism.*

Addressing the Privacy of Homeland Security-Related Information at the State Level

The National Governors Association (NGA) recognized the importance of technology and privacy in states' homeland security efforts by including in its "Domestic Preparedness Checklist" the following measures states may want to take:

- "Identify what intelligence information is needed at the state level, who can receive it, and assess security clearances with the Department of Defense and the FBI. Ensure Governor has viable statutory mechanisms in place to share intelligence information between state and local agencies and consider mandating a formal communication network between the intelligence community and medical community."
- "Examine state laws and authorities that relate to search and seizure, invasion of privacy, quarantine, evacuation, relocation or restricting access and consider enacting new health emergency powers act if necessary."
- "Review current state laws dealing with record checks, background checks, and access to public records to ensure they do not interfere with security. Consider whether legislation changes in the state's open records law are necessary to ensure the protection of sensitive documents; review information posted on websites concerning sensitive information and critical infrastructure protection."
- "Create a counterterrorism task force to identify shortfalls in legal authorities, programmatic authorities, and funding issues. Counterterrorism task forces should include Chief Information Officers and local capabilities, especially the EMTs, fire and rescue, public health and medical, public utilities, and disaster preparedness personnel whose responsibility it would be to respond to terrorist events."

View the entire NGA Domestic Preparedness Checklist at: http://www.nga.org/cda/files/DomPrepChecklist.pdf.

In order to increase security, some states have enacted laws that provide state and local law enforcement authorities with an enhanced ability to conduct electronic surveillance or to enhance the role that information technology plays in securing the U.S. For more information about such state legislative efforts, please see the National Conference of State Legislatures' (NCSL) publications "2003 Information Technology and Internet Laws" and "2003 Telecommunications Laws," which are available to registered users at: http://www.ncsl.org or for purchase via email at books@ncsl.org.

SUBSECTION C: Considerations for Privacy-Related Activities

Drafting Website Privacy Policies ::

Important Information Privacy Issue

An issue of importance for all levels of government with an Internet presence is drafting website privacy policies to inform the public of what information may be collected from them and how that information may be used or disclosed.

Considerations for Drafting Website Privacy Policies

Note that the references in this section that refer to "you" are directed to states and other entities that are developing or have website privacy policies. This section is intended to serve as a starting point for states and others in considering what information to place in their website privacy policies. We are not recommending that all of the elements listed below should be contained in your state's website privacy policy but are providing them for your consideration. You should pick and choose which ones are most suitable to address your state's website privacy policy needs.

The information contained below was compiled from a review of existing privacy policies from general state websites and portals. If you would like to view a privacy policy from a specific state, please go to www.nascio.org and click on "State Profiles." For each state profiled, NASCIO provides a link to its general state website privacy policy.

This section is organized according to the fair information use principles of the Federal Trade Commission (FTC).

1: Notice/Awareness

What information is collected:

- What types of statistical information you collect automatically. For example, types of statistical information might include:
  - *Name of the domain from which the user accessed the Internet*
  - *Date and time of access to the site*
  - *Internet (IP) address of the website from which the user directly linked to the site*
  - *Type of browser*
  - *Type of operating system*
- What mechanism is used to track statistical information, such as a server log
- Whether you obtain personally identifiable information about a user. Examples of personally identifiable information are:
  - *Name*
  - *Address*
  - *Email address*
  - *Social Security Number*
  - *Driver license number*
  - *Password*
  - *Bank account information*

- ⇨ *Credit card information*
- ⇨ *Any combination of data that could be used to identify the user, such as date of birth, zip code or gender*

- Whether you will collect any personal information without a user's consent
- Whether information will only be collected where necessary to provide services to the user
- Whether any personally identifiable information collected must be relevant to the purpose for which it is needed
- Whether the state portal (as opposed to individual websites that can be accessed through the portal) requests specific information from users

Disclosure, sale and use of collected information:

- Whether you will disclose or sell a user's personal information
- The purposes for which a user's personal information may be disclosed. For example:
  - ⇨ *For civil, criminal or administrative matters*
  - ⇨ *To protect the state's legal rights or during emergencies when physical safety is believed to be at risk*
- Whether any marketing databases are created from a user's personal information
- Whether any user profiles are created from collected personal information
- Whether any comments submitted by a user are subject to the state's online privacy policy
- How you use any statistical information collected from users without their choice, such as:
  - ⇨ *To measure the number of visitors to different sections of the website*
  - ⇨ *To help make the website useful to visitors*
  - ⇨ *To assist agencies hosted on the server in analyzing the use of their websites*
- How the personal information a user voluntarily submits will be used. For example, if a user submits an email address, the user's email address may be used for any of the following:
  - ⇨ *To respond to the user's email*
  - ⇨ *To address issues identified by the user*
  - ⇨ *To further improve the website*
  - ⇨ *To forward email to another agency for appropriate action*

Changes to your privacy policy:

- Whether and how you notify users of a change in your website privacy policy
- Whether any information collected under a previous version of your privacy policy will remain protected under that previous version or whether it is protected under the current version of your privacy policy

Public records and information:

- Whether there are state laws that generally make state government records accessible to the public
- Whether there are state laws that make confidential some types of state information, and, if so, the types of information considered to be confidential under any such laws

Other applicable laws:

- Citation of any privacy rights afforded under the state's constitution, laws or regulations

- Whether information collected online is subject to the same access and privacy laws and regulations as information collected offline
- Whether state law mandates that all agencies create and maintain an information privacy policy, and, if so, what requirements an agency must fulfill in order to implement the policy. For example:
  - ⇨ *Designation of which position within an agency is responsible for the implementation of the policy*
  - ⇨ *Prominent posting of privacy policies in agency offices and on agency websites*
  - ⇨ *Mandated distribution of the policy to agency employees and contractors*
  - ⇨ *Compliance with any state information practices and privacy and public records laws*
  - ⇨ *Use of appropriate means to implement and adhere to the privacy policy*
- Whether state contractors must comply with your state privacy policy

Use of cookies:

- What cookies do (such as an explanation that they may carry user information from one webpage to another)
- The differences between session and persistent cookies, such as differences in the duration of cookies (for example, session cookies end when a user closes his or her browser, whereas persistent cookies are of a longer duration)
- Whether your website uses one or both types of cookies
- What types of user information are collected by any cookies your website uses
- Where the information collected from cookies is stored, such as:
  - ⇨ *On the user's work station*
  - ⇨ *On the state's server*
- Whether you can delete cookies
- If cookies are not currently used on a website, whether future releases of the website will require the use of cookies
- Whether the use of cookies is mandatory to obtain services from your website

Linking from other websites:

- Whether the state encourages others to place links on their websites to your state's website
- Instructions for placing a link to your state's website on another website

Privacy of children's information:

- Whether any information submitted by a child is treated the same or differently from information submitted by an adult user
- For more information on specific concerns you may want to address through your state's privacy policy regarding the collection, use and disclosure of children's information, see the Section II of this publication.

Disclaimers:

- The general purpose of presenting information on your general state website, such as for the convenience of the reader
- That every effort is made to keep information contained on the website up-to-date
- That the state does not certify the authenticity of information that originates from third parties

- That the state does not incur any liability for any actions or omissions made in reliance on any information contained on your website regardless of the source or for any consequences from any such actions taken in reliance on information contained on your website

Relationship to other state policies:

- Whether individual state agencies and local governments that are accessible through the state portal have their own privacy policies, and, if so, whether those policies may differ from the general privacy policy on the state website
- Listing the forms of the website addresses of agencies and other websites, such as websites for the state judiciary, that may have privacy policies that differ from the state's general privacy policy
- Whether other agencies may have service delivery functions or data collection applications that may have privacy policies specifically applicable to those activities
- Notice to contact individual state agencies or local governments on the use of information contained on their individual websites

Copyright issues:

- Whether a user might encounter on your website information or documents that are protected by a copyright
- A statement that any transmission or reproduction of copyright-protected materials requires the copyright owner's permission unless otherwise allowed under the "fair use" doctrine of copyright law
- Provide a link to a discussion of what constitutes "fair use" of information under copyright law
- Whether agency-authored documents are considered to be in the public domain

Policies on external links:

- Whether there are links on your state's website to external websites or pages containing information that was created and is maintained by third parties
- Circumstances under which you place external links on your state's website, such as:
  - ⇨ *When the external link is consistent with the state's goal to serve its citizens*
  - ⇨ *Expanding users' access to information*
  - ⇨ *For the ease and convenience of the user*
  - ⇨ *Increasing the volume of high-quality government services online*
  - ⇨ *Improving customer service*
  - ⇨ *Extending city and county online services to users*
  - ⇨ *Where required or authorized by law*
- That the inclusion of external links does not constitute an endorsement of any products or services offered or referenced on the linked websites, any organizations sponsoring the external websites or any views expressed or referenced on the external websites
- That, when a user links to another website, he or she is subject to the privacy policies of that website
- Note that a state can choose to include a policy on external links in its privacy statement or make it a separate stand-alone policy

2. Choice/Consent

Generally:

- Whether the user has a choice about the collection of personally identifiable information
- The types of personal information a user may voluntarily submit to you (for example, an email address)
- How the personal information a user voluntarily submits will be used. For example, if a user submits an email address, the user's email address may be used for any of the following:
  - ⇨ *To respond to the user's email*
  - ⇨ *To address issues identified by the user*
  - ⇨ *To further improve the website*
  - ⇨ *To forward email to another agency for appropriate action*
- Whether a user has a choice of whether to receive updates and announcements from your website
- Directions for controlling cookies

Personalized portal pages:

- Whether a user has the choice of personalizing an individualized web portal page and, if so, what information is required for that, such as the user's email address or a password
- Whether a cookie is necessary in order to create a personalized portal page, and, if so, what information it collects and if any such information is stored

3. Access/Participation

Right to inspect records:

- Whether a citizen has the right under applicable law to inspect state records containing his or her personal information
- Whether a citizen has the right under applicable law to correct any inaccurate information about himself or herself

Information about the state's accessibility policies:

- Whether there are state laws or policies requiring accessibility and an explanation of any such laws or policies
- Links to any state standards on accessibility

A user's rights regarding online transactions:

- Once a user has initiated an online transaction, whether that user can then decline to proceed with the transaction at anytime prior to completion
- Whether a user can be denied a state service or benefit for declining to proceed with a transaction online
- Whether a user can transact business with the state on an in-person basis

4. Integrity/Security

- That security is a priority for the state
- What steps you take to protect a user's personally identifiable information, such as:
  - ⇨ *Certain types of technologies*
  - ⇨ *A brief description of how the state's security technologies work*
- Whether a log tracks records requests when a state employee or contractor is accessing billable or subscriber information
- Whether you audit users' access to records involving billable or subscriber services
- Whether individual state agencies may have their own security policies that could differ from the state's general website security policy
- Whether the state monitors network traffic to identify unauthorized attempts to upload or change information or cause other damage to the state network

5. Enforcement/Redress

- Who to contact if a user has questions or concerns about the website's policies
- Who to contact if a user or citizen has a concern regarding access to his or her information via the state's open records law
- Whether any attachments sent to the general comments email address for user feedback will be deleted due to security concerns regarding computer viruses

Governmental Data Matching Activities and Agreements ::

Important Information Privacy Issue

An issue of importance is the ability of government agencies to match the information they possess on individuals with that of other government agencies. These types of matching activities allow the government to collect citizens' information less frequently and assist agencies in ensuring that they have more accurate citizen information. However, government data matching activities have raised concerns that the government will create "profiles" of individuals by compiling their personal information from multiple governmental agencies. Hence, government agencies must address such concerns when performing data matching activities.

Federal Authority on the Issue

The Computer Matching and Privacy Protection Act of 1988 and Amendments of 1990 (the Computer Matching Act), 5 USC §552a(a)(8)-(13), (e)(12), (o), (p), (q), (r) & (u).

- **What Does It Do?** The Computer Matching Act amended the Privacy Act of 1974 to provide requirements federal agencies must follow when matching information on individuals with information held by other federal, state or local agencies. A federal agency must enter into a written agreement with another agency before embarking on data matching activities. Such agreements must provide a detailed account of how the information will be handled and how individuals will be notified that their information may be verified through a data matching program. The Computer Matching Act also requires that federal agencies create a Data Integrity Board and take certain measures when an individual is denied benefits based upon information obtained through a data matching program.

- **To Whom Does It Apply?** The Computer Matching Act's requirements apply to federal agencies participating in data matching activities. It does not purport to regulate the data matching activities of state or local governments, except to the extent that they participate in a data matching program with a federal agency.

- **What Elements of Control Do States Have Regarding Data Matching Agreements?** The Computer Matching Act does not regulate state or local government data matching activities unless they are matching their data with that of a federal agency. However, in instances in which a state agency participates in a data matching program with a federal agency, the state agency must enter into a written agreement with the federal agency. The federal agency's "data integrity board" monitors the state agency's compliance with the agreement. State agencies involved in a data matching program must not deny, terminate or suspend assistance under a federal program based upon information obtained through the data matching program until they have fulfilled the Computer Matching Act's notice requirement and the information has been verified or the federal agency's data integrity board has made a determination regarding the information's integrity.

Link to the Computer Matching Act as contained the Privacy Act of 1974:
http://www4. law.cornell.edu/uscode/5/552a.html [see provisions (a)(8)-(13), (e)(12), (o), (p), (q), (r) & (u)].

Application of this Privacy Issue

What Types of Information are Involved in this Issue? The Computer Matching Act applies to the sharing of federal agencies' records with other government agencies. A "record" is defined as "any item, collection, or grouping of information about an individual that is maintained by an agency," which includes (but is not limited to) the following types of information:

- Education information
- Financial transactions information
- Medical history
- Criminal history
- Employment history.

In order for the Computer Matching Act to apply, the agency records must contain an individual's name or other identifier, such as a number, symbol, finger or voice print or photo. The records also must be maintained by a federal agency in a "system of records," which is "a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

What Types of Activities are Involved in this Issue? The Computer Matching Act provides requirements for federal agencies participating in data matching programs. These types of programs involve the computerized comparison of:

- Two or more automated federal personnel or payroll systems of records
- A system of federal personnel or payroll records with non-federal records
- Two or more automated systems of records or a system of records with non-federal records to establish or verify the eligibility or compliance of beneficiaries or others with the legal requirements of federal cash or in-kind assistance benefit programs
- Two or more automated systems of records or a system of records with non-federal records to recoup payments or delinquent debts under a federal cash or in-kind assistance benefit program.

There are, however, a number of instances in which federal agencies do not have to comply with the Computer Matching Act's requirements, including:

- To produce aggregate statistical data without personal identifiers
- For research or statistical projects where the data will not be used to make decisions about specific individuals' rights, benefits or privileges
- By criminal law enforcement agencies, where the matching is performed after the initiation of a criminal or civil law enforcement investigation against an individual
- For certain tax-related purposes
- For routine administrative purposes (subject to the guidance of the Director of the Office of Management and Budget) with records relating to federal personnel
- For matching by an agency using only records from its system of records where adverse action will not be taken against federal personnel
- For foreign counterintelligence or background checks
- Incident to a levy under the Internal Revenue Code
- Pursuant to specific provisions of the Social Security Act.

Considerations for Addressing Privacy Concerns with Data Matching Activities and Agreements

The considerations below are based upon the requirements of the Computer Matching Act. The Computer Matching Act's requirements only apply to state and local governments if they are engaged in data matching activities with a federal agency. However, in determining what types of privacy protections are appropriate for data matching activities, state governments may use the requirements of the Computer Matching Act for guidance.

Data Matching Agreements:

If you enter into data matching activities with another agency, enter into a written data matching agreement.

- *This is a requirement for state and local agencies that enter into data matching activities with federal agencies.*

Elements of a data matching agreement include:

- *Purpose and legal authority for the data matching program*
- *Justification for the data matching program*
- *Anticipated results, including an estimate of any savings*
- *Description of the records to be matched, including each data element, approximate number of records to be matched, and project starting and completion dates*
- *Procedures for:*
  - ⇨ *Individualized notice at the time of application and periodically thereafter to applicants and recipients of a federal benefit program and to applicants for or those holding positions as federal personnel that any information provided may be subject to verification via a matching program*
  - ⇨ *Verifying information produced in such matching programs*
  - ⇨ *The retention and timely destruction of identifiable records created by the agency receiving records ("the recipient agency") or the non-federal agency participating in the program*
  - ⇨ *Ensuring the security of the matched records and the program's results*
  - ⇨ *The recipient or non-federal agency's use of the records, including the return of the records to the source agency or destruction of the records*
- *Prohibitions on the duplication and redisclosure of records within or outside of the recipient agency, unless required by law or where such is essential to the matching program*
- *Information on assessments that have been made on the records' accuracy*
- *A provision that the Comptroller General may have access to all records of the non-federal or recipient agency as he deems necessary to monitor or verify compliance with the agreement.*

Other requirements under the Computer Matching Act include:

- *Federal agency data matching agreements must be sent to the Senate Committee on Governmental Affairs and the House Committee on Government Operations*
- *The agreements may only last up to 18 months, but may be renewed for an additional one year if the program will be conducted without any change, and each agency certifies that it has been in compliance with the agreement.*

Data Integrity Boards:

Establish a data integrity board to oversee and coordinate the implementation of a data matching program.

- *Federal agencies conducting or participating in a data matching program are required to establish a data integrity board that consists of senior officials designated by the agency head and the agency's inspector general, if any.*

Duties of data integrity boards at the federal level include:

- *Reviewing, approving and maintaining all written data matching agreements in which the agency receives or discloses records to ensure compliance with all requirements*
- *Reviewing all data matching programs in which the agency has participated during the year, including all recurring matching programs, to ensure compliance with all legal requirements and to assess the programs' costs and benefits*
- *Submitting an annual report on the agency's matching programs to the agency head and the Office of Management and Budget (OMB) that can be made available to the public upon request*
- *Serving as a clearinghouse for receiving and providing information on the accuracy, completeness and reliability of matching program records*
- *Providing interpretation and guidance to the agency's components and personnel on a matching program's requirements*
- *Reviewing the agency's recordkeeping and disposal policies for matching programs to ensure compliance with the Computer Matching Act*
- *Reviewing and reporting on the agency's matching activities that do not constitute data matching programs under the Computer Matching Act.*

The contents of the data integrity board's report to OMB must include the following items:

- *Matching programs in which the agency has participated*
- *Matching agreements that were disapproved by the data integrity board*
- *Changes in membership or structure of the data integrity board*
- *Reasons for any waivers of a cost-benefit analysis prior to the approval of a data matching agreement*
- *Any violations of matching agreements that have been alleged or identified and any corrective actions that were taken*
- *Any other information the Director of OMB requires for the report.*

A data integrity board may only approve a data matching agreement if the program is likely to be cost-effective under a cost-benefit analysis, unless:

- *The data matching program is required by law (in which case, no cost-benefit analysis is needed), or*
- *The data integrity board determines in writing that a cost-benefit analysis is not required in accordance with guidelines established by the Director of OMB.*

If a data integrity board disapproves of a proposed data matching program, then the Computer Matching Act provides for an appeals process to the Director of OMB by any party to the proposed agreement.

Determinations Based on Adverse Information:

Government agencies (including state and local agencies) cannot suspend, terminate or reduce or make a final decision that is adverse to an individual under a federal benefits program without ensuring the integrity of the program's information upon which the decision is based by:

- *Independently verifying the adverse information, or*

- *Waiting for the data integrity board to determine that the information is limited to the identification and amount of benefits paid and that there is a high degree of confidence regarding the information's accuracy.*

Government agencies (including state and local agencies) also must comply with the following notice requirements prior to taking adverse action against an individual:

- *The individual must have received notice from the agency and have had an opportunity to contest such findings, and*
- *The time period for an individual to respond to the notice must have expired.*

Addressing Privacy Issues Regarding State Data Matching Activities and Agreements

Since the Computer Matching Act does not govern state or local governments' matching of data (unless such sharing involves a federal agency), state laws and policies govern state data matching programs. Below, you will find various approaches that a state may consider regarding data matching and other data sharing agreements.

Data Matching Privacy Issue	State	Link to State Legal Authority
Providing requirements for the contents of data matching agreements: • Minnesota has a statute that requires that, before participating in a matching program, a public entity must enter into a written agreement. The statute lists elements that data matching agreements must contain. Those elements are similar to those found in the Computer Matching Act. Wisconsin has a similar statute.	MN WI	http://www.revisor.leg.state.mn.us/stats/13B/02.html *(see §13B.02)* http://www.legis.state.wi.us/statutes/Stat0019.pdf *(see §19.69(1))*
Providing for verification of data produced in a data matching program before the termination, reduction or denial of benefits: • Minnesota has such a statute. A public entity may not take such adverse action before independently verifying the data upon which the adverse decision was based. Wisconsin has a similar statute.	MN WI	http://www.revisor.leg.state.mn.us/stats/13B/03.html *(see §13B.03)* http://www.legis.state.wi.us/statutes/Stat0019.pdf *(see §19.67)*
Providing for notice to an individual of any adverse action taken based upon information from a data matching program and of the individual's right to contest the findings: • Minnesota has a statute that contains this requirement. It also provides that its data verification requirements and its notice provisions may be satisfied "by verification, notice, hearing, and appeal rights governing the particular benefit program or employment or licensing procedures from which data were obtained to be used in the matching program." Wisconsin has a similar statute.	MN WI	http://www.revisor.leg.state.mn.us/stats/13B/03.html *(see §13B.03)* http://www.legis.state.wi.us/statutes/Stat0019.pdf *(see §19.69(3))*

Data Matching Privacy Issue	State	Link to State Legal Authority
Providing that data sharing agreements must include a provision that personal information may be used solely for the purposes of the agreement: • Washington State Executive Order 00-03 specifies this. In addition, it also requires that data sharing agreements state that personal information will not be shared with, transferred to or sold to unauthorized third parties.	WA	http://www.governor.wa.gov/eo/eo_00-03.htm.
Providing that an agency that receives personal information from another state agency must protect the information in the same manner as the agency that collected the personal information: • Washington State Executive Order 00-03 provides for this. Minnesota also has a statute that requires this.	WA MN	http://www.governor.wa.gov/eo/eo_00-03.htm http://www.revisor.leg.state.mn.us/stats/13/03.html *(see §13.03(4))*
Requiring each state agency that enters into a data sharing agreement to establish reasonable procedures to review, monitor, audit or investigate the use of personal information by contractors: • Washington State Executive Order 00-03 provides for this as well as providing that such procedures may include, when appropriate, the "salting" of such databases to detect violations of data sharing agreements.	WA	http://www.governor.wa.gov/eo/eo_00-03.htm *(see §13.03(4))*
Requiring copies of computer matching agreements be filed with the Public Records Board: • Wisconsin requires agencies that match computer data files to provide notice to the Public Records Board so these agreements may be carried in a registry.	WI	http://www.legis.state.wi.us/statutes/Stat0019.pdf *(see §19.69(2))*
Providing for sanctions in data sharing agreements where there are violations: • Washington State Executive Order 00-03 states that "[c]ontractual provisions related to breach of the privacy protection of state contracts or agreements shall include, as appropriate, return of all personal information, termination, indemnification of the state, provisions to hold the state harmless, monetary or other sanctions, disbarment, or other appropriate ways to maximize protection of citizens' personal information." Minnesota also provides its remedies under its State Data Practices Act to violations of the Computer Matching Statute. See §13B.05, 13.08 - .09 of Minnesota's public records privacy protection statutes.	WA MN	http://www.governor.wa.gov/eo/eo_00-03.htm http://www.revisor.leg.state.mn.us/stats/13B/05.html *(see §13B.05)* http://www.revisor.leg.state.mn.us/stats/13/08.html *(see §13.08)* http://www.revisor.leg.state.mn.us/stats/13/09.html *(see §13.09)*

Data Matching Privacy Issue	State	Link to State Legal Authority
Providing for requirements regarding data matching or sharing agreements in a specific context: • For example, Minnesota has a statute that governs data matching within the context of child support and maintenance obligations.	MN	http://www.revisor.leg.state.mn.us/stats/13B/06.html *(see §13B.06)*

SECTION IV. Conclusion

NASCIO hopes that this publication will serve as a foundation of knowledge upon which states can build their privacy protections and policies. In the coming years, NASCIO will continue its educational and public policy efforts on privacy. We encourage others within all levels of government as well as those in the private sector to use NASCIO as a resource for guidance and technical advice on protecting citizens' privacy now and in the future.

For more information about NASCIO's privacy efforts, please see http://www.nascio.org/hotIssues/privacy/. This webpage contains information on NASCIO's Privacy Committee as well as information about NASCIO's *Federal Privacy Law Compendium* (2003).

APPENDIX A: Privacy-Related Definitions

Subsection A: General Privacy-Related Terms

Below you will find privacy-related definitions. In providing these definitions, NASCIO's intent is to provide the reader with an explanation of terms commonly found in literature on information privacy. NASCIO recognizes that there may be alternate definitions for these terms but is providing these particular definitions for the reader's convenience.

[Note: (*) denotes definitions from the Center for Democracy and Technology's *Guide to Online Privacy*, which can be viewed at: http://www.cdt.org/privacy/guide/terms/, and (**) denotes derivation of definitions from NASCIO's Federal Privacy Law Compendium.]

- **Aggregate:** Refers to data that is combined together without releasing personally identifiable information. The statistic "70% of users of this Web site live in New York City" is an example of aggregated information.*
- **Anonymity:** A condition in which your true identity is not known. Your online service provider may allow you, as a subscriber, to participate in online activities anonymously (not known at all) or pseudonymously (taking on a different identity).*
- **Content:** The actual text of a communication or information sent. Includes text of emails, bulletin board postings, chat room communications, files and graphics. Content does not include routing information, the date, time, or subject of the message, or other transactional data.*
- **Data Element:** An individual data entity, such as last name or telephone number.*
- **Data Mining:** The practice of compiling information about Internet users by tracking their motions through websites, recording the time they spend there, what links they click on and other details that the company desires, usually for marketing purposes.*
- **Individual Profiling:** Refers to a site's or a service provider's use of personal data to create or build a record on the particular individual or computer for the purpose of compiling habits or personally identifiable information of that individual or computer. For example, online stores may recommend products based on the visitor's purchasing history on the specific website or online in general.*
- **Online Contact Information:** Information that allows an individual to be contacted or located on the Internet, such as the email address. Often, this information is independent of the specific computer used to access the network.*
- **Online Profiling:** The practice of aggregating information about consumers' preferences and interests, gathered primarily by tracking their online movements and actions, with the purpose of creating targeted advertisement using the resulting profiles.*
- **Personally Identifiable Transaction Data:** Information that describes your online activities such as the websites that you have visited, addresses to which you have sent email, files that you have downloaded, and other information revealed in the normal course of using the Internet. Transactional data differs from the content of a communication since it is not the actual substance of your communication, but rather the information about your communication.*
- **Physical Contact Information:** Information that allows an individual to be contacted or located in the physical world—such as a telephone number or an address.*

- **Security:** The fourth principle of fair information guidelines, along with (1) Notice, (2) Choice, and (3) Access. Refers to data collectors' responsibility to take reasonable steps to ensure that information collected from consumers is accurate and secure from unauthorized use. There exists a number of ways that online services can safeguard data; examples include passwords, audit trails, and encryption.*
- **Spam:** Unsolicited "junk" email containing advertising or promotional messages sent to large numbers of people.*
- **Unique Identifiers:** Non-financial identifiers issued for purposes of consistently identifying the individual. These include government-issued identifiers such as a Social Security Number, as well as identifiers issued by a website or service.*

Subsection B: Fair Information Practices Terms

- **Access:** The third principle of fair information guidelines, along with (1) Notice, (2) Choice, and (4) Security. Refers to the user's ability to view and contest the accuracy and completeness of data collected about them.*
- **Choice:** The second principle of fair information guidelines, along with (1) Notice, (3) Access, and (4) Security. Refers to companies' providing consumers with options regarding whether and how personal information collected from them may be used for purposes beyond those for which it was provided.*
- **Collection:** Online collection of personal information (i.e., shopping preferences, interests, physical contact information) occurs in two ways. First, data may be collected through your input of information, such as during a financial transaction or acquisition of a membership. Second, detailed personal information may be collected while you engage in "passive" online activity—for example, when you peek into chat rooms, glance at bulletin boards or browse through online libraries. When you ftp a file, your actions may generate a personally identifiable record. Your personal information may thus be collected and stored while you believe that you remain anonymous.*
- **Consent:** Explicit permission, given to a website by a visitor, to handle her personal information in specified ways.*
- **Correction:** User ability to alter incomplete or inaccurate personal information that a company has collected.*
- **Disclosure:** Refers to companies' practice of making your personal information available to third parties, e.g., marketing lists, other organizations that provide similar services, etc.*
- **Downstream Data Use:** Refers to companies' practice of disclosing personal information collected from users to other parties "downstream" to facilitate a transaction. For example, a content provider may disclose your personal information to a shipping company that will deliver the order to your house. The content provider may also disclose your personal information to a billing or credit card company in order to charge you for the transaction.*
- **Fair Information Practices:** Privacy guidelines, which predate the online medium, that were enumerated in the 1973 report released by the U.S. Department of Health, Education, and Welfare, which addressed privacy protections in the age of digital data collection. The principles—(1) Notice, (2) Choice, (3) Access, and (4) Security—have been developed and recognized by agencies in the U.S., Canada, and Europe.*
- **Fairness:** A goal of Fair Information Practices, which requires a company to use personal information only for the purpose for which it was initially collected.*
- **Limitation on Collection:** Refers to the established principle that collection of personal

data should be limited to information that is necessary to complete a transaction. For instance, an online service provider that requires you to provide a copy of your tax returns as a condition of becoming a subscriber obviously collects more information than it requires to process a membership. When personally identifiable information is not necessary to support the initial activity, users should have the opportunity to restrict or deny its collection.*

- **Notice:** The first principle of fair information guidelines, along with (2) Choice, (3) Access, and (4) Security. Refers to data collectors' disclosure of their information practices prior to collecting personal information from consumers. In the online context, notice means that Internet users learn from the online service provider or website whether and to what extent the service or site collects and uses their personal information.*
- **Opt In:** An option that requires your explicit consent for the use and disclosure of your personal information beyond the original, primary purpose for which it was collected. For instance, example.com may provide an empty check-box and state, "I permit example.com to share my personal information beyond the purpose for which it was collected." The company thus requires you to affirmatively consent, or opt in, before it will use or share your personal information beyond the primary purpose. The website's default program assumes that you have not consented to such use unless you check off the box.*
- **Opt Out:** An option that allows you to prevent the use and disclosure of your personal information beyond the original, primary purpose for which it was collected. For instance, example.com may display a checked-off box and state, "I permit example.com to share my personal information beyond the purpose for which it was collected." You must un-check the box, or opt out, to prevent the company from using or sharing your personal information beyond the primary purpose. The website's default program assumes that you have consented to such use unless you un-check the box.*
- **Purpose:** The reason(s) for data collection and use.*
- **Secondary Use:** Refers to using personal information collected for one purpose for a second, unrelated purpose. A fundamental fair information principle is the provision of the opportunity for a user to choose if she wants her personal information used for a secondary purpose. The principle allows you to provide personal information for a specific purpose without the fear that it may later be used for an unrelated purpose without your knowledge or consent.*
- **Transparency:** A goal of Fair Information Practices, which requires a company to inform users what personal information the company collects and how the data is used.*

Subsection C: Children's Online Privacy-Related Terms

- **Children's Online Privacy Protection Act (COPPA):** A federal law that provides general requirements for website operators to follow regarding the collection, use and disclosure of information collected from children while they are online. The law also authorizes the Federal Trade Commission to promulgate regulations to implement its requirements. It is intended to give parents a way to control the information that is collected from their children online. 15 USC §§6501-6506.**
- **Children's Personal Information:** Includes the first and last name, home and email addresses, phone number, and Social Security Number of a child under age 13. 15 USC §6501 & 16 CFR §§312.2-312.3.**
- **Websites or Online Service Directed to Children:** A commercial website or online service that is targeted to children or that portion of a commercial website or online service that is targeted to children. 15 USC §6501(10)(A).**

Subsection D: Department of Motor Vehicles Privacy-Related Terms

- **Driver's Privacy Protection Act:** A federal law that restricts the disclosure of personal information obtained by state departments of motor vehicles in connection with motor vehicle records. 18 USC §§ 2721-2725.**
- **Highly Restricted Personal Information:** Includes an individual's photograph or image, Social Security Number, and medical or disability information. The Driver's Privacy Protection Act restricts this type of information from disclosure by state departments of motor vehicles unless it is for use in one of four enumerated instances, including in connection with legal proceedings or for use by the government, by insurers for underwriting or claims investigations or by employers for verification of information about the holder of a commercial driver's license. 18 USC §2721(a)(2) & §2725(4).**
- **Motor Vehicle Records:** A record that pertains to a motor vehicle operator's permit, motor vehicle title, motor vehicle registration, or identification card issued by a state department of motor vehicles. 18 USC §2725(1).**
- **Personal Information:** Includes an individual's photograph, Social Security Number, driver identification number, name, address (but not the five-digit zip code), phone number, and medical or disability information. The Driver's Privacy Protection Act restricts this type of information from disclosure unless it falls within one or more of the statute's fourteen enumerated exceptions. 18 USC § 2721(a)-(b) & §2725(3).**

Subsection E: Health Privacy-Related Terms

- **Covered Entity:** An entity that must comply with HIPAA's provisions, including health plans, health care clearinghouses, and health care providers. Public Law 104-191 (1996).**
- **Health Insurance Portability and Accountability Act (HIPAA):** A federal law intended to standardize the electronic exchange of health information and improve the privacy and security of health information. Public Law 104-191 (1996).**
- **Privacy Rule:** A rule promulgated by the U.S. Department of Health and Human Services that regulates the disclosure and use of health information contained in medical records of HIPAA covered entities. 45 CFR §164.501 et seq.**
- **Security Rule:** A rule promulgated by the U.S. Department of Health and Human Services that standardizes the way HIPAA covered entities protect the confidentiality, integrity, and availability of electronic protected health information. 45 CFR Parts 160, 162 & 164.**
- **Transactions and Code Sets Rule:** A rule promulgated by the U.S. Department of Health and Human Services that standardizes the data content that is exchanged by HIPAA covered entities. 45 CFR Parts 160 & 162.**

Subsection F: Financial Privacy-Related Terms

- **Financial Information:** Information about an individual's finances, including account status and activity information such as account balance, payment or overdraft history, and information about an individual's purchase or use of financial instruments including credit or debit card information. Note: Purchase information alone does not constitute financial information.*
- **Financial Institution:** An institution that is significantly engaged in financial activities, which typically includes banks, savings and loans, credit unions, insurance companies, securities and commodities brokerage firms, mortgage brokers, check cashers, financial

advisors, credit counselors, and government entities that provide financial products, such as mortgages or student loans. 15 USC §6809 & 16 CFR §313.3(k)(1).**

- **Gramm-Leach-Bliley Act (Financial Services Modernization Act):** A federal law that removes the legal barriers that prevented mergers between banks, insurance companies, brokerage firms and other financial entities. It also regulates the disclosure of nonpublic personal information held by financial institutions and assesses criminal penalties against those who fraudulently attempt to gain access to individuals' financial information. 15 USC §6801 et seq.**
- **Nonpublic Personal Information:** Information which is personally identifying to the consumer and is obtained by a financial institution. 15 USC §6809.**

Subsection G: Educational Privacy-Related Terms

- **Directory Information:** Information about a student that may be made publicly accessible as long as a parent is given notice and an opportunity to let the educational institution know that the parent would like to be asked for consent before that type of information is made publicly available. Such information includes a student's name, address, phone number, date and place of birth, major, participation in school activities or sports, height and weight for students on athletic teams, dates of attendance, awards, degrees, and the most recent educational institution previously attended by a student. 20 USC §1232g(a)(5).**
- **Education Records**: Records that contain information directly related to a student and are maintained by an educational agency or institution or person acting for an educational agency or institution. 20 USC §1232g(a)(4).**
- **Family Educational Rights and Privacy Act (FERPA):** A federal law that provides privacy protection for students' education records, while ensuring a parent's rights to access his or her child's education records, correct mistakes in those records, and know who has requested or obtained the records. 20 USC §1232g.**

Subsection H: Website Privacy Policy-Related Terms

- **Cookie:** A piece of information unique to you that your browser saves and sends back to a web server when you revisit a website (the web server is the computer that "hosts" a website that your browser downloads or "sees"). The server "tells" your browser where to put the cookie on the server. Cookies contain information such as log-in or registration information, online "shopping cart" information (your online buying patterns in a certain retail site), user preferences, what site you came from last, etc.*
- **Privacy Policy:** A page or pages on a website that describe privacy policies, i.e., what personal information the site collects, how it uses it, with whom the site shares it, and whether users can exercise control over the use of their personal data.*

APPENDIX B: Major Federal Privacy Developments

This appendix details privacy-related recent events from 2000 through 2003. They are categorized according to types of information, such as medical and financial information, and also by federal entity, such as the Department of Homeland Security and the Office of Management and Budget. While this listing of recent privacy events is not intended to be exhaustive, it is intended to provide the reader with an overview of important information privacy developments since 2000.

SUBSECTION A: Privacy Developments by Types of Information ::

Children's Information Privacy

Background: *The following three statutes have been of significance in the area of children's information privacy from 2000 to 2003:*

- ***The Children's Online Privacy Protection Act of 1998 (COPPA)*** *provides parents with increased control over the information that is collected from their children online by website operators and how that collected information may be used. In 1999, the Federal Trade Commission (FTC) issued the Final Rule for implementing COPPA's provisions. For more information about COPPA, please see the FTC's website at: http://www.ftc.gov/privacy/privacyinitiatives/childrens.html.*

- ***The Child Online Protection Act (COPA)*** *provides criminal and civil penalties against those who make harmful materials available for commercial purposes to minors under age 17 via the Internet. In 1998, the American Civil Liberties Union (ACLU) filed suit in a U.S. District Court citing that COPA was unconstitutional on free speech grounds. In 1999, the court issued a preliminary injunction to prevent COPA from becoming effective. Provisions of a similar law, the Communications Decency Act of 1996 (CDA), had been struck down in 1997 by the U.S. Supreme Court as unconstitutional on grounds that it violated the First Amendment right to free speech. For more information about COPA, view the Library of Congress' Thomas website at: http://thomas.loc.gov/ (see Public Law 105-277). For more information on CDA, see the Library of Congress' Thomas website at: http://thomas.loc.gov/ (see Public Law 104-104).*

- ***The Children's Internet Protection Act (CIPA)*** *mandates that public libraries and schools cannot receive certain types of federal funding if they do not install software to filter out obscenity and child pornography on computers that are accessible to the public. For more information about CIPA, see the Library of Congress' Thomas website at: http://thomas.loc.gov/ (see Public Law 106-554).*

April 2000: COPPA and the FTC's COPPA Final Rule Go Into Effect. Website operators must obtain parental consent before the online collection of information from children under 13. View the COPPA statute at: http://www.ftc.gov/ogc/coppa1.htm. View the FTC's Final Rule for COPPA at: http://www.ftc.gov/os/1999/10/64fr59888.pdf.

June 2000: The Third Circuit Court of Appeals Upholds a Preliminary Injunction Against the Enforcement of COPA. The opinion upholds the lower court's preliminary injunction stating that, due to the current technology limitations, the ACLU's argument that COPA is unconstitutional is likely to succeed on its merits. For more information, view the court's opinion at: http://www.ca3.uscourts.gov/opinarch/991324.txt.

June 2000: The U.S. Office of Management and Budget (OMB) Directs All Federal Agencies and All Contractors Operating on Behalf of Federal Agencies to Comply with COPPA's Requirements Regarding any Websites Directed to Children. View the OMB memorandum at: http://www.whitehouse.gov/omb/memoranda/m00-13.html.

December 2000: Congress Passes the Children's Internet Privacy Act (CIPA) that Requires Filtering Software to be Used by Schools and Libraries Receiving Federal Funds. For more information about CIPA, see the Library of Congress' Thomas website at: http://thomas.loc.gov/ (see Public Law 106-554).

April 2002: The FTC Extends the Sliding Scale Provision for Obtaining Parental Consent under COPPA for Three More Years. The sliding scale provision of COPPA allows for website operators to obtain parental consent via email and an additional method of verification of consent if the child's information will not be disclosed to third parties. Stricter methods of obtaining parental consent apply where the child's information will be disclosed to third parties. According to the FTC's Final Rule on COPPA, the sliding scale provision was to expire in April 2002. View a notice of the FTC's extension at: http://www.ftc.gov/os/2002/04/67fr18818.pdf.

May 2002: A U.S. District Court Rules that CIPA is Unconstitutional on Grounds that it Violates the First Amendment. For more information, view the court's opinion at: http://www.paed.uscourts.gov/documents/opinions/02d0415p.pdf.

May 2002: The U.S. Supreme Court Keeps in Place the Preliminary Injunction Prohibiting COPA's Enforcement and Remands the Case to the Third Circuit Court of Appeals for Further Disposition. The U.S. Supreme Court comments that COPA is not unconstitutional simply because it relies on a "community standards" measure of whether material transmitted via the Internet is considered to be harmful to minors. However, the Court's decision did not address whether COPA is otherwise unconstitutionally overbroad or vague and remanded the case to the Third Circuit Court of Appeals to decide those issues. For more information, view the U.S. Supreme Court's opinion at: http://a257.g.akamaitech.net/7/257/2422/13may20021500/www.supremecourtus.gov/opinions/01pdf/00-1293.pdf.

March 2003: The Third Circuit Court of Appeals Upholds the Preliminary Injunction Against the Enforcement of COPA. The court affirms the injunction on grounds that more probably it will be proven that COPA is substantially overbroad. For more information, view the court's opinion at: http://www.ca3.uscourts.gov/opinarch/991324.pdf.

June 2003: The U.S. Supreme Court Upholds CIPA. The U.S. Supreme Court reverses a decision of a lower court that found that CIPA was unconstitutional. For more information, view the U.S. Supreme Court's opinion at: http://a257.g.akamaitech.net/7/257/2422/23jun20030800/www.supremecourtus.gov/opinions/02pdf/02-361.pdf.

Driver's Information Privacy

Background: *The Driver's Privacy Protection Act (DPPA) restricts the disclosure of personal information held by state departments of motor vehicles. The original legislation restricted the disclosure of "personal information," such as a person's name, phone number, address and Social Security Number.*

January 2000: The U.S. Supreme Court Upholds the Constitutionality of the DPPA. South Carolina and others had challenged the DPPA on grounds that it violated the constitutional principles of federalism that are inherent in the division of power between the states and federal government. However, the Court did not agree with that argument, stating that it was a proper use of Congress' authority to regulate interstate commerce and does not run afoul of constitutional principles of federalism. For more information, view a summary of the decision at Cornell's Legal Information Institute at: http://supct.law.cornell.edu/supct/html/98-1464.ZS.html.

October 2000: Congress Passes Legislation Amending the DPPA. The new legislation provides "highly restricted personal information," such as a person's photo, Social Security Number and medical or disability information, with additional protections. This type of personal information can only be disclosed without an individual's consent in a limited number of exceptions. For more information, see the DPPA as amended on Cornell's Legal Information Institute website at: http://www4.law.cornell.edu/uscode/18/pIch123.html.

Health Information Privacy

Background: *In 1996, Congress enacted the Health Insurance Portability and Accountability Act of 1996 (HIPAA) to standardize the electronic exchange of health information and improve the privacy and security of patient health information. To implement HIPAA's requirements, the U.S. Department of Health and Human Services (HHS) has promulgated several rules, including the Transactions and Code Sets Rule, the Privacy Rule and the Security Rule. The purpose of the HIPAA Privacy Rule is to establish a federal floor for the protection of individually identifiable health information. For more information on the HIPAA Privacy Rule, please view a HHS overview of the rule at: http://www.hhs.gov/ocr/hipaa/guidelines/overview.pdf or see the HHS Office of Civil Rights' HIPAA privacy website at: http://www.hhs.gov/ocr/hipaa. For more general information about HIPAA, please view the Centers for Medicare and Medicaid Services' HIPAA administrative simplification website at: http://www.cms.gov/hipaa/hipaa2/default.asp.*

August 2000: HHS Publishes the Final Transactions and Code Sets Rule for HIPAA. The Final Transactions and Code Sets Rule standardizes the electronic exchange of health information.

December 2000: HHS Publishes the Final Privacy Rule for HIPAA. The Final Privacy Rule provides for patient consent before the use or disclosure of protected health information prior to treatment.

March 2002: HHS Proposes Changes to the HIPAA Privacy Rule that Strengthen the Patient Notice Requirement and Make Patient Consent Optional. HHS states that the reason for the proposed modifications is to make sure that the Privacy Rule provides strong privacy protections without adversely impacting the quality of healthcare or access to healthcare by patients.

August 2002: HHS Adopts Changes to the HIPAA Final Privacy Rule. As modified, the Final Privacy Rule makes obtaining patient consent optional for the use or disclosure of protected health information for routine uses, such as treatment, payment or healthcare operations. However, covered entities must make a good faith effort to obtain a patient's written acknowledgement of the healthcare provider's privacy practices. Patient consent is required for non-routine uses of protected health information, such as for marketing purposes. View the Final Privacy Rule at: http://wwwbhhs.gov/ocr/combinedregtext.pdf.

February 2003: HHS Publishes the Final Security Rule for HIPAA. The HIPAA Final Security Rule standardizes the way that covered entities protect the integrity, confidentiality and availability of protected health information. The compliance deadline is April 21, 2005 (however, small health plans have until April 21, 2006 to comply). View the Final Security Rule at: http://www.cms.hhs.gov/hipaa/hipaa2/regulations/security/default.asp.

April 2003: Deadline for Compliance with HIPAA Privacy Rule Passes. Covered entities as defined by HIPAA must be in compliance with the Privacy Rule. Those qualifying as "small health plans" have an additional year to comply with the Privacy Rule.

April 2003: HHS Publishes the Interim Enforcement Rule for Civil Monetary Penalties. The Interim Enforcement Rule establishes procedures for HHS to impose monetary penalties against entities that violate HIPAA. This rule is a "first installment" of the HIPAA Enforcement Rule. Subsequent versions of the rule will have procedural and substantive provisions on the imposition of monetary penalties for HIPAA violations. The Interim Enforcement Rule expires on September 16, 2004. View the HIPAA Interim Enforcement Rule for Civil Monetary Penalties at: http://www.hhs.gov/ocr/moneypenalties.pdf.

October 2003: Deadline for Compliance with HIPAA Transactions and Code Sets Rule Passes. Covered entities that qualify as small plans or that filed for a one-year extension must be in compliance with the Transactions and Code Sets Rule. View the Final Transactions and Code Sets Rule at: http://www.cms.gov/hipaa/hipaa2/regulations/transactions/default.asp.

Financial Information Privacy

Background: *In 1999, Congress enacted the Financial Services Modernization Act, also known as the "Gramm-Leach-Bliley Act," to remove legal barriers that prevented mergers between banks, insurance companies, brokerage firms, and other financial entities. The Gramm-Leach-Bliley Act contains provisions that:*

- *Provide additional protection against the disclosure of individuals' nonpublic personal information that is collected, used and disclosed by banks and other entities in the financial services market.*
- *Assess criminal penalties against those who fraudulently attempt to gain access to individuals' financial information.*

For more information on the Gramm-Leach-Bliley Act, please visit the Federal Trade Commission's (FTC) website at: http://www.ftc.gov/privacy/privacyinitiatives/financial_rule_lr.html.

March 2000: The Federal Trade Commission Issues a Notice of Proposed Rule-Making Regarding the Gramm-Leach-Bliley Act's Financial Information Privacy Provisions. The Proposed Rule provides additional detail on what types of "financial institutions" must comply

with the Gramm-Leach-Bliley Act. It also implements provisions of the Gramm-Leach-Bliley Act that require notice to consumers in certain instances about a financial institution's privacy policies and practices and provides consumers with the ability to decline to have a financial institution disclose their nonpublic personal information to parties that are not affiliated with the financial institution. View the Proposed Rule at: http://www.ftc.gov/os/2000/02/65FR11173.pdf.

May 2000: The FTC Issues the Final Rule Regarding the Gramm-Leach-Bliley Act's Financial Information Privacy Provisions. While the Final Rule contains some changes based upon comments received by the FTC, the Final Rule still provides details about what types of "financial institutions" must comply with the Gramm-Leach-Bliley Act and implements the Gramm-Leach-Bliley Act's financial information privacy provisions. View the Final Rule at: http://www.ftc.gov/os/2000/05/65fr33645.pdf.

June 2002: Over 70% of North Dakotans Vote in Favor of Requiring Consent Before Financial Institutions Can Disclose Their Personal Information to Third Parties. This is the first time such a vote was held by a state to set financial privacy protections that are greater than the Gramm-Leach-Bliley Act.

Education Information Privacy

Background: *In 1974, Congress enacted the Family Educational Rights and Privacy Act (FERPA). It provided parents with new rights to review and correct their children's education records. View the text of FERPA on the Cornell Legal Information Institute's website at: http://www4.law.cornell.edu/uscode/20/1232g.html.*

July 2002: The U.S. Supreme Court Holds that FERPA Does Not Create an Individual Right to Sue for Violation of its Provisions. The Court holds that FERPA does not allow for the enforcement of its provisions via private lawsuits and instead is enforced by the Secretary of Education. For more information, view the U.S. Supreme Court's opinion at: http://a257.g.akamaitech.net/7/257/2422/20jun20021230/www.supremecourtus.gov/opinions/01pdf/01-679.pdf.

Freedom of Information Act Developments

Background: *The Freedom of Information Act (FOIA), which became effective in 1967, established the right of individuals to access government documents. However, it contains exceptions for certain types of information that are specified in the statute. The Electronic Freedom of Information Act Amendments of 1996 (Electronic FOIA) amended the original statute to provide that federal agencies must make certain types of documents, such as policy statements, available online in "electronic reading rooms." For more information generally about FOIA, please see the Introduction of the Department of Justice's FOIA Guide at: http://www.usdoj.gov/oip/introduc.htm. For more information about Electronic FOIA, please see information from the Department of Justice's Office of Information and Privacy at: http://www.usdoj.gov/oip/foiapost/2001foiapost2.htm.*

March 2001: The Department of Justice's Office of Information and Privacy Introduces a New Webpage, FOIA Post, to Disseminate FOIA-Related Information to Federal Agencies. It includes guidance on FOIA's administration for federal agency personnel as well

as a compilation of all FOIA decisions received by the Office of Information and Privacy. For more information about FOIA Post, please see: http://www.usdoj.gov/oip/foiapost/2001 foiapost1.htm.

March 2001: The U.S. General Accounting Office (GAO) Releases a Report on Federal Agencies' Compliance with the Electronic Freedom of Information Act. The GAO study focuses mainly on the compliance of 25 agencies. The report generally finds that the agencies had implemented many of the Electronic FOIA provisions, but still had not made all of the required categories of documents available online. View the GAO report, GAO-01-378, at: http://www.gao.gov/new.items/d01378.pdf.

October 2001: Attorney General John Ashcroft Issues a Policy Memorandum to Federal Agencies to Protect Sensitive Records that Could Implicate National Security and other Interests, such as Law Enforcement and Personal Privacy. The memorandum establishes a new standard for determining when the Department of Justice will defend challenges to agency actions that are taken under FOIA. The Department of Justice will defend agency actions under FOIA that have a "sound legal basis." The previous standard was a "foreseeable harm" standard. For more information about the memorandum, please view a summary of it as well as the memorandum itself at: http://www.usdoj.gov/oip/foiapost/2001foiapost19.htm.

March 2002: The White House Issues a Memorandum to Federal Agencies about Safeguarding Weapons of Mass Destruction Information and other Homeland Security-Related Information. The memorandum provides guidance on the matter from the Office of Information and Privacy and the Information Security Oversight Office. To view the memorandum, please see: http://www.usdoj.gov/oip/foiapost/2002foiapost10.htm.

August 2002: GAO Issues an Update to its Previous Report on Agencies' Compliance with Electronic FOIA. The report finds that progress has been made in making required documents available online as well as in the quality of annual FOIA reports by agencies. However, it also finds that FOIA request backlogs appear to be growing. For a summary of the report and a link to the report, GAO-02-493, please see: http://www.usdoj.gov/oip/foiapost/2002foiapost23.htm.

January 2003: The Homeland Security Act of 2002 Amends FOIA to Prohibit the Disclosure of Critical Infrastructure Information that is Voluntarily Submitted to the Department of Homeland Security. Significantly, for state and local governments that receive such information from the federal government, state freedom of information laws are preempted to prevent the disclosure of such information under state law. For more information from the Office of Information and Privacy, please see: http://www.usdoj.gov/oip/foiapost/ 2003foiapost4.htm.

SUBSECTION B: Privacy Developments by Federal Entity ::

Congress

Background: *Both prior to and after the September 11, 2001 terrorist attacks, there have been various measures in Congress dealing with the privacy of citizens' personal information. The listing of federal privacy bills below is not exhaustive by any means but is intended to provide the reader with a sampling of bills that NASCIO has monitored for its members.*

May 2000: Senator Gregg Introduces S 2554 "Amy Boyer's Law" to Prohibit the Display of Social Security Numbers for Commercial Purposes without an Individual's Consent. The bill was referred to the Senate Committee on Finance but was not enacted. For more information, view the bill at: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_cong_bills&docid=f:s2554is.txt.pdf.

October 2001: Congress Enacts the USA Patriot Act of 2001 in Response to the September 11, 2001 Terrorist Attacks. The law provides for enhanced investigatory tools and other measures to punish and deter terrorism. View a summary of the USA Patriot Act at: http://thomas.loc.gov/cgi-bin/bdquery/z?d107:HR03162:@@@L&summ2=m&.

April 2002: Representative Barr Introduces HR 4561, "The Federal Agency Protection of Privacy Act of 2002," to Require Federal Agencies to Assess the Impact on Individuals' Privacy when Promulgating Rules. The House of Representatives passed the bill. The bill went no further than being received in the Senate. For more information, view the bill at: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_bills&docid=f:h4561eh.txt.pdf.

December 2002: Congress Enacts "The E-Government Act of 2002" that Requires Federal Agencies to Conduct Privacy Impact Assessments. This legislation is a broad law that includes among its provisions a section that requires federal agencies to conduct privacy impact assessments before developing or procuring new IT systems that deal with individually identifiable information or before beginning a new collection of such information using IT. For more information, view the E-Government Act (see Section 208) at: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws &docid=f:publ347.107.pdf.

January 2003: Senator Feinstein Introduces S 228, "The Social Security Number Misuse Prevention Act of 2003," to Place Restrictions on the Display, Sale or Purchase of Social Security Numbers with the Owner's Consent. Representative Sweeny introduced an identical bill in February 2003, HR 637. NASCIO submitted comments on the bills, providing technical guidance on the prohibition as applied to state government. NASCIO members can view the comments on NASCIO's Washington Watch Website at: https://www.nascio.org/washwatch/. In January 2003, S 228 was placed on the Senate legislative calendar. In March 2003, HR 637 was referred to the House Subcommittee on Crime, Terrorism and Homeland Security. For more information, view S 228 at: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_bills&docid=f:s228pcs.txt.pdf.

March 2003: Senator Feinstein Introduces S 745, "The Privacy Act of 2003," to Provide Additional Protections to Financial, Health and Driver's Information as well as Social Security Numbers. The bill also would require an individual's consent before the sale of

personally identifiable information for marketing purposes. The bill was referred to the Senate Judiciary Committee. For more information, view a summary of the bill on NASCIO's Washington Watch website at: https://www.nascio.org/washwatch/congress/108.cfm#4.
View S 745 at: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_bills&docid=f:s745is.txt.pdf.

December 2003: Congress Enacts the CAN-SPAM Act of 2003, "The Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003," to Impose Limitations and Penalties on the Transmission of Unsolicited Commercial Electronic E-mail via the Internet. For more information, view a summary of the CAN-SPAM Act on NASCIO's Washington Watch Website at: https://www.nascio.org/washwatch/congress/108.cfm#7.

December 2003: Congress Enacts the FACT Act of 2003, "The Fair and Accurate Credit Transactions Act of 2003," to Address Identity Theft Concerns. The purpose of this new law is to prevent identity theft, improve the resolution of consumer disputes and the accuracy of and consumer access to credit information. For more information, view this law at: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_bills&docid=f:h2622enr.txt.pdf.

The Federal Trade Commission

Background: *The Federal Trade Commission (FTC) enforces federal consumer protection laws that prevent fraud, deception and unfair business practices. Among its areas of responsibility are financial privacy (enforcing the Fair Credit Reporting Act and the Gramm-Leach-Bliley Act) and children's online privacy (enforcing the Children's Online Privacy Protection Act). The FTC also handles complaints and other issues related to identity theft. For more information, see the FTC's website at: http://www.ftc.gov/bcp/conline/pubs/general/guidetoftc.htm.*

May 2000: The FTC Submits a Report to Congress Regarding the Enactment of Privacy Legislation to Establish Minimum Standards for the Online Collection of Information. The recommended legislation would require commercial websites that collect consumers' personal information to conform to the fair information practices of notice, choice, access and security. However, Commissioner Orson Swindle dissents from the report and Commissioner Thomas Leary issues a statement that concurs in part and dissents in part from the report. Please see the FTC's website for more information at: http://www.ftc.gov/opa/2000/05/privacy2k.htm. View the FTC's "Privacy Online: Fair Information Practices in the Electronic Marketplace" at: http://www.ftc.gov/reports/privacy2000/privacy2000.pdf.

July 2000: The FTC Settles its Complaint Against Toysmart. The FTC had filed a complaint against the company for representing that it would not share consumers' personal information with third parties and then violating that privacy policy by attempting to sell its detailed customer databases, in connection with the selling of the rest of its assets due to financial difficulties. The settlement allows for the sale of the customer information lists only as a package, including the Toysmart website, to a "qualified buyer," that is in a market related to Toysmart's market and agrees to be Toysmart's successor-in-interest to the customer information lists. For more information, view a press release at: http://www.ftc.gov/opa/2000/07/toysmart2.htm.

January 2001: The FTC Introduces Consumer Fraud and Identity Theft Data for the Public on its Consumer Sentinel Website. This statistical data was aggregated from consumer complaints. Consumer Sentinel is a one-stop, secure investigative cybertool and complaint database, on a separate restricted-access secure website, that provides hundreds of law enforcement agencies immediate access to Internet cons, telemarketing scams and other consumer fraud-related complaints. View the Consumer Sentinel website at: http://www.consumer.gov/sentinel/.

October 2001: FTC Chairman Muris said that the FTC would Increase by 50% the Resources Devoted to Protecting Privacy. Included in the FTC's privacy agenda are efforts to create a National "Do No Call" List, help identity theft victims, encourage accuracy and compliance with the Fair Credit Reporting Act, increase enforcement of children's online privacy, and enforce the Gramm-Leach-Bliley Act. For more information, view a FTC press release at: http://www.ftc.gov/opa/2001/10/privacy.htm and the FTC's privacy agenda at: http://www.ftc.gov/opa/2001/10/privacyagenda.htm.

January 2002: The FTC Reports that Identity Theft is the Top Consumer Fraud Complaint of 2001. Forty-two percent of all FTC complaints are identity theft-related. For more information, see a FTC press release at: http://www.ftc.gov/opa/2002/01/idtheft.htm.

December 2002: The FTC Announces the Creation of a National "Do Not Call" List to Allow Citizens to Stop Most Unsolicited Telemarketing Calls. Registration will be available online and by telephone. After a period of time to set up the registration process, telemarketers will be able to access the list to delete from their call lists those individuals signed up to the Do Not Call List. For more information, see an FTC press release at: http://www.ftc.gov/opa/2002/12/donotcall.htm.

January 2003: The FTC Announces that Identity Theft is the Top Category of Complaints that it Received in 2002. 43% of all complaints filed with the FTC's Consumer Sentinel Database relate to identity theft. Identity theft also was the top FTC complaint category in 2000 and 2001. For more information, view a FTC press release at: http://www.ftc.gov/opa/2003/01/top10.htm or view the FTC's "National and State Trends in Fraud and Identity Theft: January-December 2002" at: http://www.consumer.gov/sentinel/pubs/Top10Fraud_2002.pdf.

June 2003: The FTC Announces that it is Accelerating the Schedule of the Do Not Call List and Launches the Do Not Call List Registration Website. Online registration is available at donotcall.gov and telephone registration is available for consumers in states west of the Mississippi River (telephone registration will be available to those in other states in July). By the end of the month, more than 10 million telephone numbers are registered. For more information, view a FTC press releases at: http://www.ftc.gov/opa/2003/06/dncaccelerated.htm, http://www.ftc.gov/opa/2003/06/donotcall.htm, and http://www.ftc.gov/opa/2003/06/dncregistration.htm.

September 2003: The FTC Releases an Identity Theft Survey Showing 27.3 Million Victims in the Past Five Years and Billions in Losses. For more information, view a FTC press release at: http://www.ftc.gov/opa/2003/09/idtheft.htm or the FTC's "Report: Federal Trade Commission Overview of the Identity Theft Program, October 1998-September 2003" at: http://www.ftc.gov/os/2003/09/timelinereport.pdf.

September 2003: A United States District Court (Western District of Oklahoma) Enjoins the FTC from Enforcing the Do Not Call List but Congress Subsequently Enacts Legislation that Allows the FTC to Proceed with the List. The court finds that the FTC does not have the requisite authority to promulgate a national Do Not Call list. However, Congress' legislation ratifies the FTC's authority to create and implement the list. For more information about how to view the court's opinion, please see its website at: http://www.okwd.uscourts.gov/. View Congress' Do Not Call List legislation at: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ082.108.

September 2003: A United States District Court (District of Colorado) Holds that the FTC's Do Not Call List Violates Free Speech under the First Amendment. For more information about how to view the court's opinion, please see its website at: http://www.co.uscourts.gov/dindex.htm.

October 2003: The Tenth Circuit Court of Appeals Grants the FTC's Request for a Stay of the U.S. District Court's Ruling Preventing the Enforcement of the Do Not Call List. The stay on the lower court's ruling will last until the case is decided on the merits. For more information about how to view the Tenth Circuit Court of Appeals' opinions, see its website at: http://www.ck10.uscourts.gov/.

December 2003: The FTC and other Federal Agencies Issue an Advanced Notice of Proposed Rulemaking Regarding the Gramm-Leach-Bliley Act. The notice requests comments on whether the agencies should consider amending the Gramm-Leach-Bliley Act to allow or require financial institutions to provide alternative types of privacy notices that are easy to understand. Comments are due before or on March 29, 2004. For more information about the notice, please view it at: http://www.ftc.gov/os/2003/12/031223anprfinalglbnotices.pdf.

Office and Department of Homeland Security

Background: *In response to the September 11, 2001 terrorist attacks, the Bush Administration created the Office of Homeland Security (OHS) by Executive Order in October 2001. Governor Tom Ridge was appointed as Director of OHS. The mission of OHS was to develop and coordinate the implementation of a comprehensive national strategy to secure the U.S. from terrorist threats and attacks. View the Executive Order creating OHS at: http://www.dhs.gov/dhspublic/display?content=308. In November 2002, Congress enacted HR 5005, which established the Department of Homeland Security (DHS). It is the largest reorganization of government since 1947's merging of the branches of the U.S. Armed Forces into the Department of Defense. Twenty-two formerly disparate agencies will be coordinated under DHS. View HR 5005 at: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ296.107.pdf. For more information about DHS, view the DHS website at: http://www.dhs.gov/dhspublic/index.jsp.*

January 2003: The Department of Homeland Security has its First Day of Operations. For more information, see DHS's "Day One Fact Sheet" at: http://www.dhs.gov/dhspublic/display?theme=47&content=406.

February 2003: The Release of DHS's "The National Strategy to Secure Cyberspace." One of the guiding principles of the strategy is the protection of privacy and civil liberties. The strategy provides that the federal government will regularly consult with privacy advocates and

experts. It also states that the legislation that created the Department of Homeland Security also authorized the position of a chief privacy officer. View "The National Strategy to Secure Cyberspace" at: http://www.whitehouse.gov/pcipb/.

April 2003: The Department of Homeland Security Appoints its First Chief Privacy Officer, Nuala O'Connor Kelly. She is tasked with protecting the privacy and civil liberties of citizens afforded under the Constitution and US laws and ensuring that the technology used in DHS sustains and does not erode privacy protections. View a press release announcing Ms. Kelly's appointment at: http://www.dhs.gov/dhspublic/display?content=562.

July 2003: DHS Files a Notice in the Federal Register to Narrow CAPPS II's Use of Airline Passenger Information to Make Flying More Secure without Impinging on Individual Privacy Rights. CAPPS II (Computer Assisted Passenger Prescreening System) will use routine information that individuals provide when making an airline reservation (such as name, date of birth, home address and phone number) to confirm the individual's identity and assess a risk level associated with the individual. Under CAPPS II, an individual's name will be run against information in commercial databases. With the revised plan published in the notice, commercial data providers will not acquire ownership of passenger name records or retain or commercially use those records or passenger scores. In addition, CAPPS II will not use bank or medical records or records indicating an individual's creditworthiness. For more information, see a DHS press release at: http://www.dhs.gov/dhspublic/display?content=1135.

October 2003: DHS Unveils the US VISIT Program. US VISIT (United States Visitor and Immigrant Status Indicator Technology) aims to improve border management at ports of entry by capturing more complete arrival and departure data from those who require a Visa in order to enter into the U.S. One of the goals of US VISIT is to safeguard the personal privacy of visitors to the U.S. US VISIT aims to fulfill this goal by securely storing the travel information and making it available to authorized officials and selected law enforcement agencies on a need-to-know basis. For more information, view a DHS press release at: http://www.dhs.gov/dhspublic/display?content=2244 and the DHS US VISIT webpage at: http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0333.xml.

The United States General Accounting Office

Background: *As the auditing, evaluation and investigative arm of Congress, the U.S. General Accounting Office (GAO) examines the use of public funds and examines federal programs and activities to assist Congress in its oversight, policy and funding decisions. GAO issues reports and recommendations on a wide-range of issues, including government technology and information privacy issues. For more information about GAO, see its website at: http://www.gao.gov/.*

Below are some examples of GAO reports from 2000-2003. This is not intended to be an exhaustive list of GAO's reports on information privacy issues but is intended to demonstrate the types of issues that NASCIO monitors for its members.

September 2000: GAO Issues a Report Finding that 97% of Federal Government Websites Fail to Comply with the FTC's Fair Information Practices Standards of Notice, Choice, Access and Security. However, the report finds that approximately 85% of federal websites posted a privacy notice. The report also finds that only a small number of websites disclosed that they may allow third-party cookies. To view "Internet Privacy: Comparison of

Federal Agency Practices with FTC's Fair Information Principles," AIMD-00-296R, type in the report number under "Find GAO Reports" on the GAO website at: http://www.gao.gov.

March 2002: GAO Issues a Report on the Cost and Prevalence of Identity Theft. The report finds that it is difficult to track identity theft trends, because of the lack of information systems to track identity theft cases. Overall, the report finds that the prevalence and cost of identity theft appears to be growing. To view "Identity Theft: Prevalence and Cost Appear to be Growing," GAO-02-363, type in the report number under "Find GAO Reports" on the GAO website at: http://www.gao.gov.

May 2002: GAO Issues a Report on Identity Theft Statutes and their Enforcement. The report finds that, although there are federal and state laws that allow for the prosecution of identity theft, there is no centralized source for data on the enforcement of such statutes. To view "Identity Theft: Greater Awareness and Use of Existing Data Are Needed," GAO-02-766, type in the report number under "Find GAO Reports" on the GAO website at: http://www.gao.gov.

May 2002: GAO Issues a Report on Government's Use of Social Security Numbers. It finds that government agencies are taking some measures to protect SSNs, but that the safeguards are not uniformly in place at any level of government. To view "Social Security Numbers: Government Benefits from SSN Use but Could Provide Better Safeguards," GAO-02-352, type in the report number under "Find GAO Reports" on the GAO website at: http://www.gao.gov.

June 2003: GAO Issues a Report on Agencies' Compliance with the Privacy Act of 1974. GAO finds that compliance with the Privacy Act and the Office of Management and Budget's (OMB) related guidance is generally high in many areas but uneven across the federal government. GAO determines that additional guidance from OMB would help to remedy such compliance gaps.

September 2003: GAO Issues a Report on the Improved Verification of Social Security Numbers and the Exchange of States' Driver Records. GAO examines states' use of the Social Security Administration's service to verify SSNs. GAO finds that the exchange of drivers' information would help to improve the identification of individuals. To view "Social Security Numbers: Improved SSN Verification and Exchange of States' Driver Records Would Enhance Identity Verification," GAO-03-920, type in the report number under "Find GAO Reports" on the GAO website at: http://www.gao.gov.

The Office of Management and Budget

Background: *The Office of Management and Budget (OMB) assists the President in overseeing the preparation of the federal budget and supervising the administration of executive branch agencies. For more information about E-Government and OMB, please see: http://www.whitehouse.gov/omb/egov/.*

June 2000: OMB Issues a Memorandum to Federal Agencies on Privacy Policies and Data Collection on Federal Websites. The memorandum reminds federal agencies that they must establish clear privacy policies and adhere to them. The memorandum also provides a new policy for the use of cookies on federal agencies' websites and on the websites of contractors operating websites on behalf of federal agencies. Federal agencies cannot use cookies, unless,

in addition to the placement of a clear and conspicuous notice, (1) the federal agency has a compelling need to gather data from the website, (2) the federal agency uses appropriate safeguards concerning the information collected from the use of cookies, and (3) the head of the agency provides his or her approval. Finally, the memorandum also states that federal agencies and their contractors who operate websites directed at children must comply with the Children's Online Privacy Protection Act. To view the memorandum, please see: http://www.whitehouse.gov/omb/memoranda/m00-13.html.

December 2000: OMB Issues a Memorandum to Federal Agencies on the Inter-Agency Sharing of Personal Data and How to Protect Individuals' Privacy. The memorandum states that the agencies must comply with the Computer Matching Amendments to the Privacy Act of 1974. It also provides guidance on such topics as notice, content, redisclosure limitations, accuracy, security controls, minimization, accountability, and privacy impact assessments. To view the memorandum, please see: http://www.whitehouse.gov/omb/memoranda/m01-05.html.

September 2003: OMB Issues a Memorandum to Federal Agencies on Implementation of the Privacy-Related Provisions of the E-Government Act of 2003. The memorandum provides guidance on agencies' drafting of privacy impact statements, posting website privacy policies, translating privacy policies into a standardized machine-readable format, and reporting annually to OMB regarding compliance with the E-Government Act's privacy provisions. Also included in the memorandum is a summary of the Federal Trade Commission's guidance for federal agencies on complying with the Children's Online Privacy Protection Act (COPPA), which regulates website operators' online collection of children's personal information (a previous OMB memorandum requires federal agencies to comply with COPPA's requirements). The memorandum provides a summary of how it modifies previous OMB memoranda. For more information, view the memorandum at: http://www.whitehouse.gov/omb/memoranda/m03-22.html.

Information Privacy Issues Related to the Federal Courts

Background: *The Judicial Conference is the chief policy-making body for the federal courts. The U.S. Supreme Court Chief Justice is the Presiding Officer. The remainder of the Judicial Conference is comprised of judges from various levels of the federal judiciary.*

August 2001: A Committee of the Federal Judicial Conference Issues a Report Recommending Electronic Access to Case Files. The report recommends that information in civil case documents should be made available electronically with the exception of deleting Social Security Numbers from electronically available civil case documents and the redaction by litigants of certain "personal identifiers," such as financial account numbers, Social Security Numbers, dates of birth, and the names of minor children. For criminal case documents, the Committee recommends that such documents not be made available to the public electronically for two years, but that that policy recommendation can be revisited within that two year period. The Conference as a whole adopted these and other technology-related policies in September 2001. For more information, view press releases about the policies at: http://www.uscourts.gov/Press_Releases/privacyrel.pdf and http://www.uscourts.gov/Press_Releases/jc901a.pdf.

March 2002: The Judicial Conference Approves a Pilot for Remote Electronic Access to Criminal Case Filings. The Conference also amends its policy to allow for Internet access to filings in "high profile" criminal cases. For more information, view a press release at: http://www.uscourts.gov/Press_Releases/pr031302jc.pdf.

Other Information Privacy-Related Efforts of the Federal Government

The following is a brief update on some federal-level technology programs that have involved information privacy issues.

Terrorism Information Awareness Program (TIA): TIA was created under the Defense Advanced Research Projects Agency (DARPA), which is a central research and development organization for the U.S. Department of Defense (DoD). After the September 11, 2001 terrorist attacks, DARPA created TIA to research and develop an experimental prototype network in order to combat terrorism through better decision-making. It was to accomplish this goal by integrating advanced collaborative and decision support tools, language translation, and data searching, pattern recognition, and privacy protection technologies. Note that TIA originally was called the Total Information Awareness program. However, due to public concerns that the technology would be used to create dossiers on U.S. citizens, TIA renamed itself the Terrorism Information Awareness program. In 2003, Congress enacted legislation (Public Law 108-7) that prohibited providing funding to DoD for TIA, unless the Secretary of Defense reports to Congress detailed information on the funded TIA projects or the President certifies in writing that such a report is not practical and the cessation of the project would endanger national security.

For more information about TIA, see: http://www.darpa.mil/body/tia/tia_report_page.htm. For more information about Public Law 108-7, view the text of the legislation (see Division M, Section 111) at: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ007.108.

Carnivore/DCS1000: Carnivore is a program developed by the Federal Bureau of Investigation (FBI) that allows the FBI to monitor Internet communications and has the ability to intercept only those communications that are the subject of a lawful court order. In September 2000, the FBI testified before the Senate Judiciary Committee regarding Carnivore, why it is a necessary tool for the FBI and how the FBI is addressing privacy concerns raised by its use. In late 2000, the IIT Institute, under contract with the Department of Justice, issued a report on Carnivore that found that it does not invade privacy but needs additional safeguards. Finally, in early 2001, the FBI renamed Carnivore, DCS1000.

To view the FBI's September 2000 testimony, see the FBI's website at: http://www.fbi.gov/congress/congress00/kerr090600.htm.

For more information on Carnivore, see the FBI's website at: http://www.fbi.gov/hq/lab/carnivore/carnivore.htm.

APPENDIX C: Privacy-Related Organizations

NASCIO recognizes that privacy is a sensitive issue that impacts numerous individuals, governments and private sector organizations in many complex ways. Privacy-related organizations have formed around these issues. Below is a listing of some of the more prominent organizations that address privacy issues. By listing this information, NASCIO does not endorse these organizations or their policies but presents descriptions of these organizations as an educational resource. In future versions of this publication, NASCIO plans to add information on other privacy-related organizations that come to our attention.

American Association of Motor Vehicle Administrators (AAMVA)

The American Association of Motor Vehicle Administrators (AAMVA) a voluntary, nonprofit, educational organization that has a mission to develop model programs in motor vehicle administration, police traffic services and highway safety. The association serves as an information clearinghouse for these same disciplines, and acts as the international spokesman for these interests. It represents the state and provincial officials in the United States and Canada who administer and enforce motor vehicle laws.

- Link to AAMVA: http://www.aamva.org/.

American Bar Association (ABA)

The American Bar Association (ABA) is a voluntary professional association for those in the legal profession. The ABA's Science and Technology Law Section includes a number of committees that address such issues as e-law privacy and privacy and computer crime.

- Link to the ABA: http://w3.abanet.org/home.cfm.

American Civil Liberties Union (ACLU)

The American Civil Liberties Union (ACLU) supports civil liberties in a wide-range of contexts from religious freedom, prisoners' rights and rights of the poor. It also addresses technology-related privacy issues, such as Internet privacy, government surveillance, and medical privacy.

- Link to ACLU: http://www.aclu.org/.

Americans for Computer Privacy (ACP)

Americans for Computer Privacy (ACP) is a broad-based coalition that brings together more than 100 companies and 40 associations representing financial services, manufacturing, telecommunications, high-tech and transportation, as well as law enforcement, civil-liberty, pro-family and taxpayer groups. It supports policies that advance the rights of American citizens to encode information without fear of government intrusion and advocates the lifting of export restrictions on U.S.-made encryption products. ACP also supports policies that promote industry-led, market-driven solutions to critical information infrastructure protection and opposes government efforts to impose mandates or design standards, or to increase widespread monitoring or surveillance.

- Link to ACP: http://www.computerprivacy.org/.

Center for Democracy and Technology (CDT)

The Center for Democracy and Technology (CDT), based in Washington, D.C., seeks to promote democratic values and constitutional liberties in the digital age, to find practical solutions to enhance free expression and privacy in global communications technologies, and to build consensus among stakeholders. Regarding Internet privacy, CDT works for individual privacy on the Internet through public policy development and technological tools that give people the ability to take control of their personal information online and make informed choices about the collection, use and disclosure of personal information.

- Link to CDT: http://www.cdt.org/.

Coalition for Sensible Public Records Access (CSPRA)

The Coalition for Sensible Public Records Access (CSPRA) is a non-profit, sponsor-supported organization, dedicated to preserving responsible commercial use of public records data. Although CSPRA supports open access to public records, they welcome all views and support in-depth discussions on privacy-related issues.

- Link to CSPRA: http://www.cspra.org/.

Electronic Frontier Foundation (EFF)

The Electronic Frontier Foundation (EFF), based in San Francisco, California, is a non-profit, donor-supported membership organization that seeks to protect and defend citizens' rights regardless of technology and works to educate the press, policymakers and the public about civil liberty issues related to technology. Among their various activities, EFF advises on legislation, initiates and defends court cases to preserve individuals' rights, launches global public campaigns, and produces proposals, papers, educational events, and an archive of digital civil liberties information.

- Link to EFF: http://www.eff.org/.

Electronic Privacy Information Center (EPIC)

The Electronic Privacy Information Center (EPIC), located in Washington, D.C., is a public interest research center that was established in 1994. EPIC's goal is to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values. EPIC publishes an online newsletter, reports and books on privacy, open government and free speech.

- Link to EPIC: http://www.epic.org/.

Global Privacy and Information Quality Working Group (GPIQWG)

The Global Privacy and Information Quality Working Group (GPIQWG) assists government agencies, institutions, and other justice entities in ensuring that personal information is appropriately collected, used, and disseminated within integrated justice information systems. The GPIQWG addresses accuracy and reliability issues involved in updating criminal history records with subsequent events (e.g., prosecution, adjudication) when those events cannot be linked to an arrest notation previously entered into the criminal history repository. This work includes exploring biometric technologies and addressing the privacy and information quality issues these technologies present. GPIQWG is a working group of the Global Justice Information Sharing Initiative.

- Link to the GPIQWG: http://it.ojp.gov/topic.jsp?topic_id=55.

Health Privacy Project

Founded in 1997, the Health Privacy Project (HPP), a non-profit corporation based in Washington, D.C., is dedicated to raising public awareness of the importance of ensuring health privacy in order to improve health care access and quality, both on an individual and a community level. It provides healthcare stakeholders with the information and tools to work more effectively toward greater protection of health information through research studies, policy analyses, Congressional testimony, extensive work with the media, and a website.

- Link to HPP: http://www.healthprivacy.org/.

International Association of Privacy Professionals (IAPP)

The International Association of Privacy Professionals (IAPP) is the result of the recent union of the Privacy Officers Association (POA) and the Association of Corporate Privacy Officers (ACPO). IAPP is an association for privacy and security professionals that helps its members build and maintain privacy programs while effectively navigating the rapidly changing regulatory and legal environments.

- Link to IAPP: http://www.privacyassociation.org/index.html.

National Association of Attorneys General (NAAG)

The National Association of Attorneys General (NAAG) is the association of the state attorneys general that was founded in 1907. NAAG addresses a broad range of issues, including such technology-related issues as Internet consumer protection and computer crimes.

- Link to NAAG: http://www.naag.org/.

NACHA-The Electronic Payments Association

NACHA—The Electronic Payments Association is an organization that develops electronic solutions to improve the payments system. NACHA represents more than 12,000 financial institutions through direct memberships and a network of regional payments associations, and 650 organizations through its industry councils. NACHA develops operating rules and business practices for the Automated Clearing House (ACH) Network and for electronic payments in the areas of Internet commerce, electronic bill and invoice presentment and payment (EBPP, EIPP), e-checks, financial electronic data interchange (EDI), international payments, and electronic benefits transfer (EBT). NACHA's mission is to promote the development of electronic solutions that improve the payments system for the benefit of its members and their customers.

- Link to NACHA: http://www.nacha.org/.

National Electronic Commerce Coordinating Council (NECCC)

In 1998 the National Electronic Commerce Coordinating Council (NECCC) was formed in an effort to build on the success of the Conference on Electronic Commerce held in 1997. The group's initial goal was to facilitate cooperation between states and the private sector as the industry moved toward electronic commerce. Associations that are included in NECCC are NASACT (National Association of State Auditors, Comptrollers and Treasurers), NASS (National Association of Secretaries of State), NIGP (National Institute of Governmental Purchasing, Inc.), AGA (Association of Government Accountants), ITAA (Information Technology Association of America), NACHA (National Automated Clearing House

Association), and NAGARA (National Association of Government Archive and Records Administrators). NECCC currently has a working group that addresses identity management issues.

- Link to NECCC: http://www.ec3.org/index.htm.

Online Privacy Alliance

The Online Privacy Alliance is a group of more than 30 global corporations and associations that facilitates business-wide actions to promote trust and foster the protection of individuals' privacy online. The Online Privacy Alliance supports self-regulatory initiatives that foster privacy online and in electronic commerce and has created a set of online privacy guidelines that member organizations must commit to follow. Link to Privacy Guidelines: http://www.privacyalliance.org/resources/ppguidelines.shtml.

- Link to the Online Privacy Alliance: http://www.privacyalliance.org/.

Privacy Exchange

Privacy Exchange, based in New Jersey, is an online global resource for consumer privacy and data protection laws, practices, issues, trends, and developments worldwide. It focuses on consumer relationships with business and industry in credit, consumer reporting, financial services, insurance, telecommunications, health and medical, pharmaceutical, information services and direct marketing. Citizen to government relationships are not typically addressed by Privacy Exchange. Privacy Exchange was founded in 1987 by two non-profit organizations, the Center for Social and Legal Research (CSLR) in New Jersey and the American Institute of Contemporary German Studies (AICGS) in Washington D.C.

- Link to Privacy Exchange: http://www.privacyexchange.org/.

Privacy International

Privacy International is a human rights group that was formed in 1990 and is based in London, England, and has an office in Washington D.C. It serves as a watchdog on surveillance by governments and corporations. Privacy International has conducted worldwide campaigns on issues such as wiretapping and national security, ID cards, video surveillance, data matching, police information systems, medical privacy and freedom of information and expression.

- Link to Privacy International: http://www.privacyinternational.org/index.html.

Progress and Freedom Foundation (PFF)

The Progress and Freedom Foundation (PFF), a non-profit organization founded in 1993, is a market-oriented think tank that studies the digital revolution and its implications for public policy. Its mission is to educate policymakers, opinion leaders and the public about issues associated with technological change, based on a philosophy of limited government, free markets and individual sovereignty.

- Link to PFF: http://www.pff.org/.

Disclaimer

NASCIO makes no endorsement, express or implied, of any links to websites contained herein, nor is NASCIO responsible for the content of the activities of any linked sites. Any questions should be directed to the administrators of the specific sites to which this publication provides links.

While NASCIO has made all reasonable attempts to ensure that the information contained in this publication and links to other information are correct, NASCIO does not represent or guarantee the correctness of the information contained herein or any linked information presented, referenced or implied. All critical information should be independently verified.