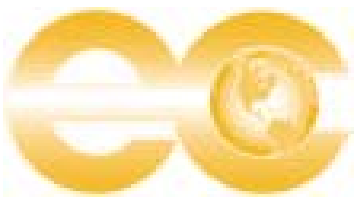
Privacy Policies – Are You Prepared?

A Guidebook for State and Local Government

Version III

NECCC
December, 2000



National Electronic Commerce Coordinating Council

The National Electronic Commerce Coordinating Council (NECCC) is an alliance of national state government associations dedicated to the advancement of electronic government within the states. The Council is comprised of **NASIRE** (a group representing the chief information officers of the states), the National Association of State Purchasing Officials (**NASPO**), the National Association of State Auditors, Comptrollers and Treasurers (**NASACT**) and the National Association of Secretaries of State (**NASS**). In addition to these voting members, other governmental and private organizations participate in an advisory capacity. These associations include the National Governors Association (**NGA**), the National Association of State Chief Administrators (**NASCA**), the Information Technology Association of America (**ITAA**) and the National Automated Clearing House (**NACHA**). The ITAA and the NACHA specifically represent private information technology companies and the financial services and technology industries.

EXECUTIVE BOARD

Chair: **Hon. J.D. Williams**, NASACT, Idaho State Controller
Vice Chair: **Richard B. Thompson**, NASPO, Maine Director of State Purchasing
Secretary/Treasurer: **Carolyn Purcell**, NASIRE, Executive Director, Texas Department of Information Resources

NECCC BOARD

NASIRE	**George Boersma**, CIO & Deputy Director, Michigan Department of Management & Budget
	Steve Kolodney, Director, Washington Department of Information Services
NASPO	**Dave Ancell**, Director, Office of Purchasing, Michigan Department of Management & Budget
	Joyce Murphy, Director, Division of Purchasing & Materials Management, Missouri Department of Administration,
NASS	**Hon. J. Kenneth Blackwell**, Ohio Secretary of State,
	Hon. Elaine Marshall, North Carolina Secretary of State
	Hon. Ron Thornburgh, Kansas Secretary of State
NASACT	**Hon. David Heineman**, Nebraska State Treasurer
	Hon. Thomas Wagner, Delaware Auditor of Accounts
NGA:	**Thom Rubel**, National Governors Association
NASCA	**Pam Ahrens**, Director, Idaho Department of Administration
ITAA	**Basil Nikas**, CEO, iNetPurchasing.Com
NACHA	**William Kilmartin**, Vice President, American Management Systems - AMS

NECCC CONTACT

Brandon W. Lenoir, Director • 202-624-5451 • e-mail: blenoir@nasact.org • web: www.ec3.org

ACKNOWLEDGEMENTS

Co-Chairs:

Basil Nikas – Board Member NECCC, ITAA Representative to NECCC, CEO iNetPurchasing.com
Eric Seabrook – Secretary of State's Office, Ohio

Researcher, Writers and Coordinators for the"Privacy Policies" Guidebook:
Jerry Johnson – T exas
Marshall High – Idaho
Danielle Germain – ITAA

Revisions and Updates Provided by:
Brandon W. Lenoir – NECCC
Jerry Johnson – Texas
Angela Babcock – Idaho
Individual State Input

Table of Contents

4 INTRODUCTION

5 ORIGINS OF THE PRIVACY DEBATE

10 RESPONDING TO CITIZEN CONCERN

14 BEST PRACTICES, MODELS AND TEMPLATES

17 PRIVACY POLICIES: WHICH STATES HAVE THEM AND WHAT DO THEY SAY

22 SUMMARY OF STATE PRIVACY POLICY ANALYSIS

23 CONTRACTING FOR WEB DEVELOPING AND HOSTING SERVICES

24 A WORD ON INTERNET SECURITY

25 LINKS AND OTHER RESOURCES

30 APPENDIX I: State Portal and Privacy Policy URL List

32 APPENDIX II: Web Privacy Assessment

NECCC PRIVACY 2000 WORKGROUP MEMBERS

Introduction

For nearly half a century, the "Big Brother" syndrome of George Orwell's chilling classic 1984, has created a concern that governments are constantly amassing information on its citizens for "nefarious" purposes. Cold War, East Bloc nations did in fact suffer abuses of state-sponsored "information gathering" - an episode in history that reaffirmed Orwellian predictions.

In extreme contrast, the United States has led the charge to protect the privacy rights of citizens through legislation such as the Freedom of Information Act. We are one of the few nations in the world that does not have "national identity cards."

Today, however, "information privacy" is being threatened by technology advancing so rapidly, legislators can scarcely keep pace. Right now, any individual or group can essentially invade and examine databases containing personal information that most Internet-users believe is privately held. As the ability to retrieve information electronically is becoming easier, new security concerns are arising such as the potential for personal information to not only be accessed, but mined and distributed, as well. The world's citizens are no longer in fear of a governmental "Big Brother," but now face a global "Virtual Big Brother."

Over the past few years, the changing nature of privacy as a result of the World Wide Web has incited much debate over the precautionary measures needed to safeguard the individual's right to privacy. Much progress has been made nationally and internationally to adopt guidelines that protect privacy, yet remain flexible enough to allow for the continued growth and development of the Internet. However, in the rush to adopt e-commerce applications on the state and local government level, the privacy debate has received minimal attention despite citizen concerns to the contrary.

The National Electronic Commerce Coordinating Council (NECCC) believes it is crucially important to raise awareness and foster discussion on the issue of on-line privacy due to the unique role states and localities play in collecting, maintaining and disseminating constituent data. The emerging networked world provides opportunities for government leaders to offer improved services while saving taxpayer dollars. Most citizens are embracing these revolutionary changes and are petitioning for even more government services to be available on-line. However, herein this citizen campaign lays the privacy paradox.

The NECCC has taken the initiative to create this guidebook to serve as a resource for state and local government officials so they may more fully understand the need to proactively address this issue. The purpose of the guidebook is to reinforce the importance of privacy policies and explain the components necessary to create an effective document. Additionally, the "Privacy Policies Guidebook" is intended to help officials to avoid potential pitfalls and hurdles by providing resources, references and other support.

Origins of the Privacy Debate

The issue concerning consumer data and the manner in which it is being collected and used by web merchants and private and government entities has caused concern that personal data, unbeknownst to the individual, is no longer personal, or protected. Although the web was originally designed for one-way data transfer, organizations quickly found a way to reverse the flow of information. Today, this technology is simplifying the ability for websites to collect personal data.

For public sector policy officials, the debate over on-line privacy has created a double-edged sword. On one side is the need to ensure fair information practices, a concern policy-makers share with the private sector. The challenge here is to guarantee laws and practices imposed on the private sector are also being followed in the public sector (the "practice what you preach" mentality). On the other side, one unique to the public sector, is the necessity to fulfill Freedom of Information obligations. How does a government entity strike the right balance between the duel responsibilities of ensuring the availability of public records while still protecting personal information? There are no easy answers to either of these questions.

At the commercial level, private industry has been an active promoter of the self-regulatory model, which has gained general acceptance by the United States government. However, the European Union (EU) has questioned the adequacy of this model. While the EU tends to favor mandating privacy laws within its borders, the European Union and the United States have been working to find mutually agreeable "safe harbor principles" which would not hinder international commerce for virtual or traditional companies.

Domestically, since the mid 1990's, the US Federal Trade Commission (FTC) has accepted the self-regulatory model. However, in 1998, the Commission did publish a set of guidelines to establish parameters for self-regulation to continue. The most significant of these regulations is the requirement web sites post "Privacy Policies or Statements," information which explains the site. Following the FTC regulations for private industry, the White House decided federal agencies should also comply with such guidelines advocating privacy policies. Therefore the Executive Office of the President directed all federal departments and agencies to post clear privacy policies on all principle web sites containing personal information collected from the public by a September 1, 2000, deadline. Any other major entry points and web pages containing similar personal data were required to comply by December 1.

The "2000 Online Privacy Survey," an FTC-commissioned study, reviewed the nature and substance of privacy disclosures on U.S. commercial websites. In Fair Information Practices in the Electronic Marketplace (web address), a report produced in May 2000, the FTC analyzed the results of the survey and determined legislation is necessary to ensure further implementation of fair information practices online, and recommended the framework for such legislation. In a 3-2 decision, FTC members found "self-regulatory initiatives to date fall short of broad-based implementation of effective

self-regulatory programs" and "such efforts alone cannot ensure that the online market place will emulate the standards adopted by industry leaders."

Similarly, Texas adopted a rule, effective July 1, 2000, requiring the home pages of all state web sites and those of any new or changed key public entry points, to include privacy policies which address the following:

- Use of server logs and/or cookies
- Information collected by other technologies and processes
- Information collected via e-mail and web-based forms. A web-based form shall post a link to the policy. The form may include a provision for the individual to opt-out of sharing the information with another party, or a warning that the information may be a public record and therefore subject to the Texas Public Information Act.
- Web pages designed for children must comply with all applicable federal and state laws intended to protect minors.
- State agencies shall plan on implementing P3P (Platform for Privacy Preferences Project) on the home page and key public entry points to a state agency Web site.
- Prior to providing access to information or services on a state Web site that requires user identification, each state agency shall conduct a transaction risk assessment, and implement appropriate security and privacy safeguards. At a minimum, state Web sites that require a citizen to enter the following information shall use an SSL session or equivalent technology to encrypt the data:

    - Both the individual's name and other personal information, such as an Social Security Number;
    - Transaction payment information; or
    - An individual's identification code and password.

(Texas rule can be found at http://www.state.tx.us/Standards/S201-12.htm)

In April 2000, the Governor of Washington issued an Executive Order to ensure state agencies protect confidential personal information to the maximum extent possible while complying fully with the state's public disclosure and open government laws. The following is a summary of the key areas covered in the Executive Order:

- Agencies that operate Internet web sites must have privacy policies that are prominently displayed on their home pages. The policies must be consistent with the Model Privacy Notice developed by the Department of Information Services.
- Agencies must establish procedures and practices for handling and disposing records that contain confidential personal information so that the information does not get into the wrong hands.
- Social Security numbers, which are key personal identifiers used in identity theft, should be removed from documents that could be subject to public scrutiny. Bank account and credit card numbers of citizens used in the electronic transfer of funds must also be kept confidential, in accordance with law (Ch. 56, Laws of 2000).

- Personal information must not be sold and lists of individuals must not be released for commercial purposes. The collection of personal data should be limited to that which is needed for legitimate public purposes and retained only as long as necessary.
- Agencies that enter into contracts or agreements for sharing personal information with other entities must have contractual requirements that protect the information from inappropriate uses.
- When personal information about citizens is collected, they should be notified that the law may require it to be disclosed as a public record. People should be informed about how they can review their personal information and recommend corrections if it is inaccurate or incomplete.
- Agencies must have contact persons to deal with privacy complaints and questions from the public.

In September, Washington state published a preliminary report on the initial results of the Executive Order and agency actions that is available for review at: http://www.governor.wa.gov/recpriv/recprivcont.htm. The model privacy policy notice developed by the Washington Department of Information Services, is available at: http://www.wa.gov/dis/e-gov/architecture/FinalPrivacyModel.htm

Several states have formed Privacy commissions or task forces to address the issues associated with the types of information that may be required for disclosure as a public record and the contracts or agreements applicable to state agencies for sharing personal information with other entities.

The results of the push to post privacy policies, in both the commercial and public sphere, have exceeded expectations. A Georgetown University study released in May of 1999 surveyed a random sample of 364 of the top 7,500 most visited "dot com" websites. Of those sites, 65.7 percent had a privacy policy posted. Similarly, all federal government agencies complied with the Office of Management and Budget directive by the required deadlines.

Some state agencies also provide special web pages for children. However, not all pages comply yet with the Children's Online Privacy Protection Act of 1998 (COPPA) (http://www.ftc.gov/os/1999/9910/64fr59888.htm), which went into effect on April 21, 2000. This Federal Trade Commission rule applies to operators of websites or online service directed at children and to operators of web sites or online services who have actual knowledge that the person from whom they seek information is a child. The requirements include:

1. To post prominent links on their websites to a notice of how they collect, use, and/or disclose personal information from children;
2. With certain exceptions, to notify parents that they wish to collect information from their children and obtain parental consent prior to collecting, using, and/or disclosing such information;
3. Not to condition a child's participation in online activities on the provision of more personal information than is reasonably necessary to participate in the activity;

4. To allow parents the opportunity to review and/or have their children's information deleted from the operator's database and to prohibit further collection from the child; and
5. To establish procedures to protect the confidentiality, security, and integrity of personal information they collect from children.

As directed by the COPPA, the FTC rule also provides a safe harbor for operators following commission-approved self-regulatory guidelines. The NECCC strongly encourages states with a "children's page" on their website to review their site to ensure compliance with COPPA.

Two other platforms or technical specifications being devised are the Platform for Privacy Preferences Project (P3P) and the Platform for Internet Content Selection (PICS). P3P is a standard developed by the World Wide Web Consortium that enables Web sites to list privacy practices in a format that can be retrieved automatically and interpreted easily by user agents. P3P agents will allow users to be informed of site practices (in both machine and human-readable formats) and to automate decision-making based on these practices when appropriate. In June, the World Wide Web Consortium conducted an interoperability demonstration that gave companies the opportunity to unveil new P3P prototypes and test them with other services. Currently, over 20 web sites are using P3P, including several federal sites and one state site, the Texas Tech University Health Sciences Center. The complete list of sites is available at http://www.w3.org/P3P/compliant_sites.

The Platform for Internet Content Selection is a set of technical specifications that enable users to easily find appropriate content and avoid content they consider inappropriate or unwanted, either for themselves or their children. These specifications were designed to ease the creation of, and access to, labeling schemes (and associated content selection and filtering mechanisms), which allow various people or organizations to classify Web content to best suit their own different viewpoints. The PICS specifications provide ratings on a web site's content.

Despite the above measures and advancements, concerns about privacy and misuse of personally identifiable information continue to grow. Despite two recent surveys conducted by the Center for Democracy and Technology and Business Week demonstrating most people do not feel their personal information has been compromised on-line. The Business Week/Harris Poll released in the March 20, 2000 edition of Business Week, had some interesting results:

- 77% of those surveyed read a site's privacy policy at least some of the time.
- 96% of those surveyed felt it was at least somewhat important that a site have a privacy policy. Of that group, 25% felt it to be absolutely essential.
- Given a choice, 56% of Internet users say they would "opt out" and not allow personal information to be collected.
- 74% say they would be uncomfortable with the sale of information to other organizations

•67% believe sharing information so individuals could be tracked across multiple sites is also inappropriate.

These findings demonstrate privacy on a website, whether it belongs to a commercial vendor, individual, or government entity, is a serious concern among American citizens.

Based on the importance Internet users place on privacy policies, The NECCC Privacy Workgroup hypothesized states and localities would be forcibly advocating the use of privacy policies on all their government run websites and portals. Unfortunately, in testing the theory, it did not prove true.

In a report released September 15, 2000, Brown's Taubman Center for Public Policy and American Institutions examined 1,813 web sites, and based on 27 different features, ranked the sites on a 100-point scale. The survey included 1,716 state government sites, 36 federal legislative or executive sites, and 61 federal court sites. A key finding of the report concluded, "only 5 percent of government websites show some form of security policy and 7 percent have a privacy policy. Ten states, or one-fifth of all states, do not have any privacy feature at all." The full report is available at: http://www.insidepolitics.org/egovtreport00.html.

In a similar, more focused study, the NECCC reviewed the main web pages or portals of the 50 states and U.S. territories, the 25 largest U.S. cities and counties based on population. In March of 2000, only 10 states (or 20%) had privacy policies that were easily accessible from their home page. A follow-up survey completed on December 1, 2000 showed that 24 states have privacy policies or notices posted, an increase of 140% in just over six months. Unfortunately, the cities and counties did not show as significant an augmentation in their numbers as the states did. Previously, no city had a privacy policy on their home page. Currently, only San Diego has added one. The largest counties (all with populations over 1.1 million people) did not yield many privacy policy postings either. In March, only Maricopa County, Arizona, had a privacy policy link on their home page. As of December 1, 2000 Maricopa is still the only county to have a privacy policy listed. Policies were absent on the remaining 24 sites.

The absence of broad adoption of privacy statements by state and local governments was a surprise to the NECCC and the members of the Privacy Workgroup as noted by the hypothesis at the start of the study. These findings seem to identify a gap between what citizens desire and what policy makers are providing. The paradigm shift from the industrial era to the information age has heightened the awareness of the average citizen about the collection and handling of their personally identifiable information. The question, now, becomes, "How will government officials address these concerns?"

Responding to Citizen Concern

The NECCC encourages state and local governments to immediately evaluate privacy issues and develop policies that respond to their citizens' privacy concerns, before privacy becomes such a major issue that it could severely impede further progress in e-government. Posting a privacy policy would be a first step in reassuring citizens that information they regard as sensitive in nature will not be improperly used, strengthening consumer support for new, innovate e-government applications and on-line services.

Private citizens tend to simplify their privacy issues into four basic questions:

- What information is collected about me?
- Is the information accurate?
- How is this information used?
- Is the information I provide shared with other parties and if so, with whom?

The comfort level of the user is determined by how effectively a privacy policy answers these questions.

The Federal Trade Commission has taken the four basic questions of citizens and established "Fair Information Principles" as a tool for developing standards in data collection. The "Principles" focus on four specific areas:

1. Notice: Data collectors must disclose their information practices before collecting personal information from consumers.
2. Choice: Consumers must be given options with respect to how personal information collected from them may be used for purposes beyond those for which the information was provided and whether they wish to have that information shared.
3. Access: Consumers should be able to view and contest the accuracy and completeness of data collected about them.
4. Security: Data collectors must take reasonable steps to ensure that information collected from consumers is accurate and secure from unauthorized use.

Taking the FTC's "Fair Information Principles" a step further, and based on the self-regulatory guidelines crafted by the Online Privacy Alliance (http://www.privacyalliance.org). The NECCC encourages states to pursue policies for protecting individually identifiable information on all of their portals, web pages and other sites of entry on the World Wide Web. The content of such policies should at a minimum address the following five points:

1. Adoption of a Privacy Policy

Each state and local government should adopt a privacy policy and take responsibility for enforcing it among its divisions and departments. Thoughtful

consideration should be given to the parameters for the policy as well as its legal implications before it is posted.

2. NOTICE AND DISCLOSURE

A privacy policy must be easy to find, read and understand. The policy should inform the constituent that when personal information is collected, there will be a limited way that information will be used, possible third party distribution of that information and the choices available regarding collection, use, and distribution of the collected information.

The policy should have a statement of the organization's commitment to data security and what steps the organization takes to ensure data quality and access. Also included, should be a clear statement of what accountability mechanism the state uses as well as contact information and the date on which the policy was last reviewed. The policy should be written with clear language that will be easily understood by the target audience. Legal jargon or other language that confuses citizens seriously undermines the usefulness of privacy policies. Policies must be available before and during the time any individually identifiable information is requested or collected.

3. OPT IN/OPT OUT CLAUSES

Many consumer protection groups have advocated for opt in or opt out clauses. These groups, along with many individuals in the public and private sector, believe that citizens should be given the opportunity to choose how their personally identifiable information collected from them on-line is used when it is unrelated to the purpose for which it was provided. The growing belief is that one of the best ways to protect privacy on the Internet is to combine the elements of opt-in and opt-out clauses.

With opt-out situations, the site is free to gather and sell information unless an individual specifically tells them not to. Opt-in, by comparison, forbids selling or gathering information unless a user gives the site permission. Opt-in and Opt-out options are usually found on sites and in places where personally identifiable information is collected and involves clicking on a box by the user.

(Note: Some state freedom of information laws precludes an agency from offering an opt-in or opt-out clause. Based on these state laws information that is collected is classified as a record and must be treated in a manner consistent with their state laws.)

4. DATA SECURITY

State entities and their affiliated agencies that collect data on-line have a unique responsibility to their constituent to ensure that the individually identifiable information collected is protected from loss, misuse, inaccuracies or alteration. Reasonable steps should be taken to ensure that third parties who receive information are aware of these

security practices and that those parties are also taking precautions to safeguard the authenticity of any transferred information.

5. DATA ACCESS

Organizations creating, maintaining, using or disseminating individually identifiable information should take precautions to assure that the data is accurate, complete and timely for the purposes for which it is to be used. States should develop mechanisms so that inaccuracies in data such as contact information, etc., may be easily corrected. These processes need to be simple, easy to use, and provide verification to the citizen that the inaccuracies have been corrected. Procedures should also be implemented to protect against accidental or unauthorized alteration of one's information.

From testimony given by consumer advocates and representatives from industry at various privacy hearings in congress this year it seems many citizens may be under the wrong impression that the Fair Credit Reporting Act of 1970 also protects them in the online world. This unfortunately is not the case. While the Fair Credit Reporting Act gives individuals the right to inspect their credit records and find out why they were denied their application for credit, there is no easy method or similar legal provision at the citizen's disposal in the networked world. While technology may exist to facilitate the retrieval of an individual's data in a database, oftentimes, data is located in various databases and not easily accessible.

On the international stage, Privacy International and the Electronic Privacy Information Center has issued their own principles in a report entitled, "Privacy & Human Rights 1999" (http://www.privacyinternational.org/survey). The following is an excerpt from that report.

"The Council of Europe's 1981 Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data and the Organization for Economic Cooperation and Development's Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data articulate specific rules covering the handling of electronic data. The rules within these two documents form the core of the Data Protection laws of dozens of countries. These rules describe personal information as data that are afforded protection at every step from collection to storage and dissemination. The expression of data protection in various declarations and laws varies in degree. All require that personal information must be:

- Obtained fairly and lawfully
- Used only for the original specified purpose
- Adequate, relevant and not excessive to purpose
- Accurate and up to date
- Accessible to the subject
- Kept secure and
- Destroyed after its purpose is completed.

The NECCC has developed a self-assessment tool that will allow agencies to administer an evaluation of the quality of their privacy policies. Titled, **State & Local**

Government Web Assessment Using the NEC3 Privacy Guide & Accessibility Standards, the tool covers many of the key points the NECCC has outlined as key elements in developing a privacy policy. After an agency administers the self-assessment they will receive a number score that rates the quality of their policy. The tool is intended to assist agencies in their effort to improve existing policies, and to aid agencies that are developing a policy. The Self-Assessment Tool can be found in *Appendix II* of this document.

Best Practices, Models, and Templates

PRIVACY POLICY

A privacy policy should be published on every government web site, even if the site does not create records of the information collected. A privacy statement should explain how information is managed. Because state agency web sites have many different purposes, the privacy policies found on these sites should also be diverse and specific to the visited site. A "one size fits all" approach to developing a privacy policy will not effectively or accurately reflect the information gathered by individual agencies or how they process and store this information.

Specific web-based forms that require personal information should post a privacy policy, or a link to the policy, at the top of the page/form indicating how the information will be used and under what conditions the information may be shared or released to another party. The form may include a provision for the individual to opt-out of sharing the information with another party, or a warning that the information may be a public record and subject to an open records request. Web pages designed for children must comply with all applicable federal (i.e., Children's Online Privacy Protection Act) and state laws intended to protect minors.

INTRODUCTORY LANGUAGE

The policy should identify the agency and include a short overview of privacy practices and how they apply to the site.

Example: The (agency name) maintains the web site as a public service. The following is the privacy policy for this site (use www.state.(domain name).us):

INFORMATION COLLECTED AND STORED AUTOMATICALLY

In the course of operating a web site, certain information may be collected automatically in logs or by cookies. Some agencies may be able to collect a great deal of information, but, according to policy, choose to collect only limited information. In some instances, agencies may have the technical ability to collect information and later take additional steps to identify people, such as looking up static Internet Protocol addresses that can be linked to specific individuals. Regardless of an agency's decision to collect this type of information or take further steps to gather more information, the privacy statement must clearly denote the policy. It is imperative to ensure these policies are consistent with the state's Freedom of Information or Open Records laws.

Example: We do not use cookies to collect information. Note: A cookie file contains unique information a web site can use to track such things as passwords, lists of pages you've visited, and the date when you last looked at a specific page or to identify your session at a particular web site. A cookie is often used in commercial sites to identify the items selected for a specific shopping cart application.

(Note: If the site uses cookies, the policy should identify what information is collected and how that information is used and protected. The main home page and privacy policy page should not require the visitor to accept, or set, a cookie.)

For site management functions, information is collected for analysis and statistical purposes. This information is not reported or used in any manner that would reveal personally identifiable information and will not be released to any outside parties unless legally required to do so in connection with law enforcement investigations or other legal proceedings.

We use Log analysis tools to create summary statistics, which are used for purposes such as assessing what information is of most interest, determining technical design specifications, and identifying system performance or problem areas. The following information is collected for this analysis:

- User Client hostname - The hostname (or IP address if DNS is disabled) of the user/client requesting access.
- HTTP header, "user-agent" - The user-agent information includes the type of browser, its version, and the operating system it's running on.
- HTTP header, "referrer" - The referrer specifies the page from which the client accessed the current page.
- System date - The date and time of the user/client request.
- Full request - The exact request the user/client made.
- Status - The status code the server returned to the user/client.
- Content length - The content length, in bytes, of the document sent to the user/client.
- Method - The request method used.
- Universal Resource Identifier (URI) - The location of a resource on the server.
- Query string of the URI - Anything after the question mark in a URI.
- Protocol - The transport protocol and version used.

INFORMATION COLLECTED FROM E-MAILS AND WEB FORMS

Many websites receive identifiable information from e-mails or web forms. It is appropriate for statements to explain how the identifiable information is treated when the individual provides it.

Example: If you send us an electronic mail message with a question or comment that contains personally identifying information, or fill out a form that e-mails us this information, we will only use the personally identifiable information to respond to your request and analyze trends. We may redirect your message to another government agency or person who is in a better position to answer your question.

SECURITY, INTRUSION, DETECTION LANGUAGE

Many agencies use information collected on a site to detect potentially harmful intrusions and to take action once an intrusion is detected. In some situations, the policy of the agency may be to not collect personal information from IP logs, for example. In

the event of authorized law enforcement investigations, however, and pursuant to any required legal process, information from those logs and other sources may be used to help identify an individual.

Example: For site security purposes and to ensure that this service remains available to all users, this government computer system employs software programs to monitor network traffic to identify unauthorized attempts to upload or change information, or otherwise cause damage.

Except for authorized law enforcement investigations, no other attempts are made to identify individual users or their usage habits. Raw data logs are used for no other purposes and are scheduled for regular destruction in accordance with electronic records retention schedules.

Unauthorized attempts to upload information or change information on this service are strictly prohibited and may be punishable under the (identify the specific state code or law).

Privacy Policies: What States Have Them and What Do They Say?

When the NECCC first began the analysis of state privacy policies in March of 2000 only ten states had a policy posted on their web site. By December 01, 2000, 24 states provided a privacy policy. Upon first observation, the review committee recognized the different levels of complexity among state policies. However, after more in-depth review, the committee did observe specific distinctions between information that may be collected simply by visiting and using a site and information given by the user in the course of conducting business via a site.

An example of the first type of information collection includes server logs showing which pages were accessed when and how, cookies that could connect separate Internet sessions and allow for an integrated profile to be created, or other "anonymous" information such as search words that are used or data typed into a tax estimator. The second type of information collection includes information users provide in order to receive a service, such as name, address, and payment information when applying for a license, checking an eligibility status or paying a ticket.

Concerning information gathered when a site is simply visited, a majority of state privacy policies clearly declare that state entities do not personally identify visitors nor do they share gathered statistical information, including customer feedback, inside or outside the state's governing bodies. Most policies use language crafted to reassure users that they can surf the state web site anonymously and without fear of leaving their personal footsteps in cyber-land. Cookies and server logs therefore, take on a less ominous role.

It is the handling of the second type of information, that which is shared in the course of web-based transactions, which is less certain. States have a vast array of policies, some intricately set out and others generalized.

When a user provides their e-mail address as part of a request for information, updates personal information, or conducts a web-based transaction, personal information is being transmitted and received by the government agency. Because such information may or may not be used, stored, or even available to web site administrators, this type of information often finds itself outside the parameters of the stated web site privacy policies. From a user perspective, however it is just this type of information, though excluded from the privacy policies, which raise the most concern over the handling of and access to this information. Consequently, governments must be more judicious in paying attention to the methods for managing transactional information and more specific in describing their policies in order to effectively bolster consumer confidence and be an advocate for conducting business on-line.

Using the two types of information outlined above as a benchmark, the NECCC analyzed the language of some of the state privacy policies to discuss and evaluate current sites and how their policies address these issues. [1]

ALABAMA, MINNESOTA AND TEXAS: WHAT'S MISSING?

All three of these states have privacy policies that address, to some extent, the types of-information they collect and how it is used. A common vein running through these policies is the collection of data in order to analyze traffic to the website and then retrieve statistics that assist states in making improvements to the site. They do not personally identify visitors to the website. However, what these three state sites do not touch upon, is how personal information, willingly provided by the visitor, is handled and whether it is shared or sold.

Alabama

As stated above, Alabama's privacy policy stresses that the site does not identify specific users. While it does use cookies to track sessions, these cookies are anonymous and temporary. The site also mentions the use of server logs that record the accessing domain, date and time, and linking website name for statistical purposes only. The policy ends with the following statement:

"We want to be very clear: *We will not obtain personally identifying information about you when you visit our site*, unless you choose to provide such information to us."
(http://www.state.al.us/info-new/privacy.html)

Minnesota

Minnesota's privacy policy, still in draft form, concisely states:

"North Star [the name of Minnesota's portal] collects information only to analyze traffic patterns and to perform routine system maintenance. We do not use the system logs or other records for any other purpose, nor do we sell, rent or otherwise improperly disclose this information. North Star does not use 'cookies'."
(http://www.state.mn.us/privacy.html)

Texas

The privacy statement for the Texas site is perhaps the best of this group because it is very clear and precise. Although the site does not use cookies, it clearly defines cookies. It explains exactly what types of statistical (server log) information it collects and also

[1] Disclaimer: This document's analysis of individual states' privacy policies, is in no way a criticism by the NECCC of the privacy-policy development efforts undertaken by state governments. The policies that are described to be "least complete" are generally the first policies to have been developed and posted. Alabama and Minnesota, for example, were the first two states to have posted privacy policies. These policies were posted in the fall of 1997, more than a year before the next two states: Washington and Iowa. Generally speaking, the policies that evolved most recently are more robust than the early ones. A lesson that can be drawn from this is that privacy policies should be revisited from time to time to make sure that they reflect the most clear and up-to-date expressions of the issues around on-line privacy.

provides a link to the analysis. Because Texas provides their Web trends analysis, citizens are able to understand what traffic analysis means. The policy also explicitly discusses how email is handled and sometimes redirected; as well as clearly and convincingly describes its data collection techniques and limits.

IOWA, VIRGINIA, MAINE, UTAH AND IDAHO: TAKING IT A STEP FURTHER

Iowa, Virginia, Maine and Utah extend the scope of their privacy policies beyond those already mentioned. These states discuss the use of cookies and server logs in tracking visitors to their sites, as well as public records laws, and how these affect the availability of personal information users provide on-line.

Iowa

To illustrate the difference in the language used in these policies, the following is an excerpt from the IOWAccess website.

"The information collected should only be that which is necessary to provide the information or services sought by a requester, just as a person might provide such information when visiting a governmental office in person. The information collected is subject to the same controls and uses as that collected by governmental offices visited in person, again subject to the access and confidentiality provisions of Chapter 22, or to other applicable sections of the Code of Iowa. You do not have to provide personal information to visit IOWAccess Web sites or download information . . . . No marketing databases are created nor is any commercial use made of any such data. Government agencies may request personally identifiable information from you in order to provide requested services, but such information is handled as it would be on an in-person visit to a governmental office. (http://www.state.ia.us/main/privacy.html)

This explanation of how information is collected by IOWAccess is strengthened by the detail given in the description of the information that is available through the site:

"Access to personally identifiable information in public records at state and local levels of government in Iowa is controlled primarily by Chapter 22 of the Code of Iowa, the law on EXAMINATION OF PUBLIC RECORDS (OPEN RECORDS). Information generally available under Chapter 22 - and not made confidential elsewhere in the Code of Iowa - may be posted for electronic access through IOWAccess. (While Chapter 22 sets the general policies for access to government records in the State of Iowa, other sections of the Code of Iowa as well as other federal laws deal with confidentiality issues.)" (http://www.state.ia.us/main/privacy.html)

Iowa seems to have the clearest description of how user provided information is handled - essentially as though the information had been collected in an office visit.

Virginia

Virginia's privacy policy is especially interesting and has several portions worthy of consideration. Virginia's portal (VIPNet) is a state-controlled authority. VIPNet includes the following description of the use and disclosure of information:

"We collect, retain and use personal information about our customers only when they volunteer to subscribe to a VIPNet premium service. We only collect, retain and use personal information where we believe it is essential (and allowed by law) to administer our business and to provide products, services and other opportunities requested by our customers."

"We do not sell or rent our subscribers' information to any outside company or organization. We do not reveal specific information about subscribers or other personally identifiable data to unaffiliated third parties for their independent use, except if required to do so by the Virginia Freedom of Information Act or other law."
(http://www.vipnet.org/vipnet/privacy.html)

A challenge many states face when developing privacy policies is how to balance the intent of the agency's desire to protect information that may become public record. Such information might be disclosed in accordance with a Freedom of Information or public record act. The VIPNet policy goes as far as to discuss security precautions, maintenance of record accuracy, and the limits and controls placed on employee access to information.

The following is another excerpt concerning access to the information collected:

"Our network manager is instructed to limit employee access to personally identifiable information to only those employees who need access in order to perform their assigned duties. The network manager is instructed to enforce with its staff their responsibilities in protecting subscriber's information."

(http://www.vipnet.org/vipnet/privacy.html)

This statement is unique in that it acknowledges and addresses the special protections that a citizen needs in cases where information is collected and potentially accessible by third parties.

Maine

Maine's privacy policy describes and explains the use of both the statistical information that is collected, as well as personal information that is provided by its web site visitors. The Maine policy also hints at the records retention issue with respect to e-mail addresses, when it says:

"The message with the sender's name and e-mail address will be saved for a period of time and then destroyed."

(http://www.state.me.us/disclaimer.html)

Maine's policy also describes the management of information provided to InforME, Maine's Internet gateway providing certain types of web-enable transactions.

"The Information Resource of Maine collects, retains and utilizes personal information about its customers only when they volunteer to subscribe to InforME. The information is used to administer subscriber accounts and to provide products, services and other opportunities requested by InforME subscribers are confidential and may only be released with the express written permission of the subscriber pursuant to the provisions of 1 MRSA Chapter 14."

(http://www.state.me.us/disclaimer.html)

Utah

Utah's privacy policy, like others, addresses the collection and handling of "anonymous" and "provided" information. It also has a particularly good section describing how e-mail addresses are treated:

"E-mail addresses obtained as a result of a request to the state site will not be sold or given to other private companies for marketing purposes. The information collected is subject of the access and confidentiality provisions of Chapter 2, other applicable sections of the Utah Code or federal law. E-mail or other information requests sent to the state web site may be maintained in order to respond to the request, forward that request to the appropriate agency, communicate updates to the state page that may be of interest to citizens, or to provide the state web designer with valuable customer feedback to assist in improving the site. Individuals will be provided with the ability to "opt out" at anytime of any communications regarding new service updates."

(http://www.state.ut.us/privacy.html)

Idaho

Idaho's privacy policy is very similar in nature to Utah's and the same analysis would apply. (http://state.id.us/privacy.html)

Summary of State Privacy Policy Analysis

The analysis of the privacy polices described here should not be interpreted as an endorsement. Instead, the review of the 8 states that were included should be viewed as a reference point for other state and local governments preparing to develop their own privacy policies. By providing examples of policies already posted by government agencies, the NECCC is remaining true to their mission of helping government avoid "re-inventing the wheel."

The NECCC analysis of the 19 states that currently have policies posted yielded varying results, and highlighted the different ways states have chosen to address the privacy issue. Some states were very concise, while others left a lot of room for interpretation. Appendix 1 provides a list of the state portals visited with their URL and also provides the link to the site privacy policy in the event a policy was posted and available.

The NECCC, in coordination with the Privacy Workgroup, will continue to update this document. The goal of the NECCC is to eventually recognize all 50 states and U.S. Territories as having posted privacy policies that meet or exceed the recommendations contained in this document. To assist in this effort, the NECCC is working to develop a "Self Assessment" tool for government agencies to use when evaluating existing privacy policies, and as a template for agencies that are in the process of developing a policy. A scoring system is being developed that will allow an agency to understand how thorough their policy is compared to other agencies within their state, as well as agencies from other states. This tool, available in December, will also be appropriate and useful for local governments and the private industry. Informing individuals of the types of information that is collected and how it is being used, will help increase trust, ensuring the viability and continued use of the Internet as a vehicle to provide services.

Contracting for Web Development and Hosting Services

The ever-changing technology and cost to retain high tech employees has lead many governments to embrace the new concept of public/private partnerships to obtain technology and services from the vendor community to electronically deliver information to their citizenry. Several states have turned to this form of out tasking web site development and hosting services to "portal" vendors as a solution. There are numerous potential benefits of this approach for vendors including the following:

- Supply web-based interfaces to existing applications;
- Offer a common interface to applications using the portal;
- Provide an electronic payment system for public payments to the government;
- Reduce, over the long term, duplicate data collection through the identification of common information shared across government entities and creation of a single login for all government applications using the portal.

However, potential drawbacks do exist.

By today's trends, public sector portal initiatives are being funded by "value-added" service transactions fees whereby in most cases, there is no cost to the agency for development, implementation and operation of this service and the supplier is compensated by these fees paid by the citizen.

In the nascent version of this model, the supplier offered the service at no cost to the public sector in return for the sale of the information collected by third parties. This collection of data by the state portal by a non-governmental private sector firm raised concerns over the ownership of the data. The Supreme Court decision earlier this year, based on a similar use of personally identifiable information in South Carolina, judged that this use of citizen data was not to be resold.

Some states contracting with vendors have passed legislation dictating the agreement does not dissolve the state's ownership of information captured by their portal even when the vendor collects the data.

It is also important the contract ensures the privacy policies set by agencies or state or federal law will be enforced and followed. The contractor should be required to provide a link to the privacy policy on all main entry pages and from any page where personal information is collected. It is strongly recommended that vendors be directed to include provisions for individuals to opt-in, opt-out and/or correct information on-line. The privacy policy should include a clear and prominent hyperlink directing visitors to the Federal Trade Commission (FTC) Web site to view educational material on consumer privacy. Currently, the FTC site contains a brochure entitled: "Site-Seeing on the Internet" which can be found at:
http://www.ftc.gov/bcp/conline/pubs/online/sitesee/index.html.

It is also recommended that the contractor be reviewed on a quarterly or semiannual audit, conducted by an independent third party, reviewing and evaluating its security and privacy practices and policies.

A Word on Internet Security

States and local governments must remember that although privacy laws are usually hard to enforce, it is up to each governing body to maintain the integrity of their privacy policy. This requires taking precautions and safeguarding data repositories against hackers and other breaches. Public confidence in the use of the Internet does not exclude concerns over information collected by a government entity. Any organization that tracks the number of "hits" received by a site is collecting personal data about the visitors to that site. In 1999 The NECCC published the "Electronic Payments Primer" that included a section on "Privacy & Security Issues." (http://www.ec3.org) This section provides an update of security risks and addresses privacy issues when contracting for web site development and hosting services.

SECURITY RISKS

In recent months, the media has covered a plethora of Internet security breaches. The following examples are meant to illustrate some pitfalls.

- In 1999, the Federal Computer Incident Response Capability (FedCIRC) received reports of 580 incidents involving 1,496,268 hosts. This was a 221% increase over the previous year.

- Last year, an intruder broke into CD Universe's computers, stole up to 300,000 credit card numbers and demanded that the site pay a "ransom" of $100,000. When CD Universe refused, hundreds of the credit card numbers were posted on the Internet. A similar incident occurred with Visa Europe.

- Early this year, MSNBC was able to view nearly 2,500 credit card numbers and other data essentially by browsing e-commerce web sites using a commercially available database tool rather than a Web browser. Not only were the sites storing the credit cards in plain text in a database connected to the Web, the databases were using the default user name and in some cases, no password. A Russian software company found the security flaws. In addition to the credit card numbers, MSNBC was able to view a wide selection of personal data including billing addresses, phone numbers and in some cases, employee Social Security numbers. Identity theft is caused by the availability of this type of information.

- The U.S. Government Accounting Office issued a report entitled "Identity Fraud" in 1998 that shows a 16-fold increase of identity theft from 1992 to 1997. As of August 1999, Trans Union, a credit-reporting bureau, was receiving about 1900 calls a day from victims of identity theft. The Internet is becoming a key resource for identity thieves. Some web sites even sell people's Social Security numbers (see http://www.infoseekers.com).

- In September, the House Banking Committee held a hearing on H.R. 4311: The Identity Theft Prevention Act of 2000. In the opening statement of Congressman Steven C. LaTourette, he stated, "complaints about identity fraud have gone up 1,400 percent since the early 1990s. The FTC is now getting 1,000 calls a week about identity theft. The Secret Service, meanwhile, says that losses to individuals whose cases they investigated jumped 75 percent from 1995 to 1997, from $442 million to $745 million. Those skilled in the Internet will undoubtedly make identity theft even more common. The bold new frontier will spark bold new criminals (see http://www.house.gov/banking/91300lat.htm).

Not only are the tools used by hackers becoming more sophisticated, some information brokers are actively seeking specific types of data they will pay hackers to obtain.

"No computer or networked system can be one-hundred percent attack proof and the job of securing a system against an illegal intrusion will never be complete. But using best practices and recommended security measures can move us forward to a more secure environment for securing the nation's infrastructures."

National Infrastructure Protection Center (NIPC), October 1998

The *"NECCC Electronic Payments Primer,"* released last year, identifies two key security areas within a risk chain: protecting data in transit and in repose by addressing the security of transaction information. A government web site that collects information about an individual when they visit, or conducts a transaction, must have security policies and procedures that protect the information. However, because the loss of government web development and security staff to the private sector is becoming common, government decision makers are being forced to look for private sector help. *(A copy of the NECCC Electronic Payments Primer can be obtained at http://ec3.org)*

Links and Other Resources

IMPORTANT FEDERAL GOVERNMENT LINKS

- Privacy of Individually Identifiable Health Information - The U.S. Department of Health and Human Services is developing "Standards for Privacy of Individually Identifiable Health Information," that will be phased in starting in 2002. State agencies that handle health care information will need to monitor and plan for implementing the security and privacy standards. Violations of the HHS regulations are subject to fines, up to $250,000. Additional information is available at: http://aspe.hhs.gov/admnsimp/index.htm

- In December 1999, the Federal Trade Commission established the "Advisory Committee on Online Access and Security" (http://www.ftc.gov/acoas). Providing consumers access to information collected about them and providing security for such information are two of five core fair information practice principles described in the Commission's 1998 report, Privacy Online: A Report to Congress. The other three principles are "Notice," "Choice," and "Enforcement."

- Federal agencies must protect an individual's right to privacy when they collect personal information, as required by the Privacy Act, 5 U.S.C. 552a, and OMB Circular No. A-130, "Management of Federal Information Resources." State and local laws vary and may protect some data items (e.g., social security number), however other information collected could be viewed as "open records." State and local government organizations need to consult with their legal counsel to ensure they can protect the information collected.

- In September, the GAO published report on "Internet Privacy: Comparison of Federal Agency Practices with FTC's Fair Information Principles" (GAO/AIMD-00-296R available at http://www.gao.gov/new.items/ai00296r.pdf). On-line privacy has emerged as one of the key and most contentious issues surrounding the continued evolution of the Internet. The World Wide Web requires the collection of certain data from individuals who visit web sites such as Internet address in order for the site to operate properly. However, collection of even this most basic data can be controversial because of the public's apprehension about what information is collected and how it could be used. As of July 2000, of the 65 web sites surveyed collected personal identifying information from their visitors, and 85 percent of the sites posted a privacy notice. The majority of federal sites (69 percent) met FTC's criteria for Notice. However, a much smaller number of sites implemented the three remaining principles Choice (45 percent), Access (17 percent), and Security (23 percent). Finally, a small number of sites (22 percent) disclosed that they may allow third-party cookies; 14 percent actually allowed their placement.

- White House http://www.whitehouse.gov/WH/html/privacy.html
- Social Security http://www.ssa.gov/privacy.html
- Internal Rev. Svc. http://www.irs.gov/prod/news/efoia/priv-pol.html
- Census Bureau http://www.census.gov/main/www/policies.html#privacy
- Immigration & Nat. http://www.ins.usdoj.gov/graphics/privnote.htm

AUDIT REQUIREMENTS

- Agencies that collect extensive data about an individual, or sensitive data (e.g., medical), should have documented policies and practices that can be audited. The Texas State Auditor's Office has published Electronic Commerce Risks and Controls http://www.sao.state.tx.us/ec.pdf.

- The CPA Web Trust (http://www.aicpa.org/webtrust/tocb.htm) form can assist agencies in assessing the type of information collected, how that information is protected, and audited.

- The NECCC audit guidance workgroup will publish an audit guide for state and local government at the annual conference in December. The document will include an audit guidebook and a risk assessment model. Following its December release a copy of the document will be posted on the NECCC Web page http://ec3.org.

STATE GOVERNMENT PRIVACY POLICY LINKS (MAIN PORTAL PAGE)

UPDATED DECEMBER 01, 2000

1. Alabama http://www.state.al.us/info-new/privacy.html
2. Arkansas http://www.state.ar.us/access.html#Privacy
3. Connecticut http://www.state.ct.us/privacy.htm
4. Florida http://www.myflorida.com/myflorida/privacy.html
5. Georgia http://www.state.ga.us/index/privacy.html
6. Hawaii http://www.state.hi.us/#
7. Idaho http://www.state.id.us/privacy.html
8. Iowa http://www.state.ia.us/main/privacy.html
9. Kansas http://www.state.ks.us/public/about-ink/privacy.html
10. Kentucky http://www.kydirect.net/kyprivacy.htm
11. Maine http://www.state.me.us/disclaimer.html
12. Maryland http://www.state.md.us/privacy.html
13. Minnesota http://www.state.mn.us/privacy.html
14. Mississippi http://www.state.ms.us/its/msportal.nsf/privacy?OpenPage
15. New Jersey http://www.state.nj.us/privacy.html
16. North Carolina http://www.ncgov.com/asp/subpages/privacy_policy.asp
17. North Dakota http://discovernd.com/privacy.html
18. Ohio http://www.state.oh.us/ohio/privacy.htm
19. Pennsylvania http://www/state.pa.us/PAPower/pages/privacy.asp
20. Tennessee http://www.state.tn.us/privacy.html
21. Texas http://www.state.tx.us/Siteinfo/privpol.html
22. Utah http://www.state.ut.us/privacy.html
23. Virginia http://www.vipnet.org/vipnet/privacy.html
24. Washington http://access.wa.gov/siteinfo/pdpnotice.asp

CITY AND COUNTY GOVERNMENT PRIVACY POLICY LINKS

- Seattle, WA http://www.ci.seattle.wa.us/terms.htm
- Maricopa County, AZ http://www.maricopa.gov/default/disclaimer.asp
- King County, WA http://www.metrokc.gov/terms.htm

CERTIFICATION PROGRAMS

These third-party programs provide "seals of approval" or "trustmarks" that provide easy recognition to consumers that minimum privacy and security standards have been met.

- TRUSTe http://www.truste.org/webpublishers/pub_principles.html
- BBBOnline http://www.bbbonline.org/businesses/privacy/eligibility
- PrivacyBot http://www.privacybot.com/eligibility_standards.shtm
- CPA Webtrust http://www.cpawebtrust.org

RESOURCES ON ONLINE PRIVACY ISSUES

These resources provide extensive information on the subject on online privacy, privacy policies, and issues regarding information and data in the information age.

- Center for Democracy and Technology http://www.cdt.org/
- Privacy Rights Clearinghouse http://www.privacyrights.org/
- Electronic Privacy Information Center http://www.epic.org/
- Electronic Frontiers Foundation http://www.eff.org/
- ACLU Cyberliberties http://www.aclu.org/
- Computer Professionals for Social Resp. http://www.cpsr.org/
- Online Privacy Alliance http://www.privacyalliance.org/
- PrivacyRatings.org http://www.privacyratings.org/
- Federal Trade Commission/Privacy http://www.ftc.gov/privacy/
- Privacy.net http://privacy.net/
- Privacy International http://www.privacy.org/pi/
- Internet Privacy Coalition http://www.privacy.org/ipc/
- Privacy Commissioner of Canada http://www.privcom.gc.ca/

Appendix I

State Portal & Privacy Policy URL List

(As of December 01, 2000)

State	Main Portal Privacy Policy URL
Alabama	Main Portal: http://www.state.al.us/ Privacy Policy: http://www.state.al.us/info-new/privacy.html
Alaska	Main Portal: http://www.state.ak.us/ No Privacy Policy Link
Arizona	Main Portal: http://www.state.az.us/ No Privacy Policy Link
Arkansas	Main Portal: http://www.state.ar.us/ Privacy Policy: http://www.state.ar.us/access.html#Privacy
California	Main Portal: http://www.state.ca.us/ No Privacy Policy Link
Colorado	Main Portal: http://www.state.co.us/ No Privacy Policy Link
Connecticut	Main Portal: http://www.state.ct.us/ Privacy Policy: http://www.state.ct.us/privacy.htm
Delaware	Main Portal: http://www.state.de.us/ No Privacy Policy Link
Florida	Main Portal: http://www.myflorida.com/myflorida/home.html Privacy Policy: http://www.myflorida.com/myflorida/privacy.html
Georgia	Main Portal: http://www.state.ga.us/ Privacy Policy: http://www.state.ga.us/index/privacy.html
Hawaii	Main Portal: http://www.state.hi.us/ Privacy Policy: http://www.state.hi.us/# *unable to access, under review
Idaho	Main Portal: http://www.accessidaho.org/ Privacy Policy: http://www.accessidaho.org/privacy.html
Illinois	Main Portal: http://www.state.il.us/ No Privacy Policy Link
Indiana	Main Portal: http://www.state.in.us/ No Privacy Policy Link
Iowa	Main Portal: http://www.state.ia.us/ Privacy Policy: http://www.state.ia.us/main/privacy.html
Kansas	Main Portal: http://www.state.ks.us/ Privacy Policy: http://www.state.ks.us/public/about-ink/privacy.html
Kentucky	Main Portal: http://www.state.ks.us/ Privacy Policy: http://www.kydirect.net/kyprivacy.htm
Louisiana	Main Portal: http://www.state.la.us/ No Privacy Policy Link
Maine	Main Portal: http://www.state.me.us/ Privacy Policy: http://www.state.me.us/disclaimer.html

Maryland	Main Portal: http://www.state.md.us/ Privacy Policy: http://www.state.md.us/privacy.html
Massachussetts	Main Portal: http://www.state.ma.us/ No Privacy Policy Link
Michigan	Main Portal: http://www.state.mi.us/index_ie.htm No Privacy Policy Link
Minnesota	Main Portal: http://www.state.mn.us/ Privacy Policy: http://www.state.mn.us/privacy.html
Mississippi	Main Portal: http://www.state.ms.us/its/msportal.nsf?Open Privacy Policy: http://www.state.ms.us/its/msportal.nsf/privacy?OpenPage
Missouri	Main Portal: http://www.state.mo.us/ No Privacy Policy Link
Montana	Main Portal: http://www.state.mt.us/ No Privacy Policy Link
Nebraska	Main Portal: http://www.state.ne.us/ No Privacy Policy Link
Nevada	Main Portal: http://www.state.nv.us/ No Privacy Policy Link
New Hampshire	Main Portal: http://www.state.nh.us/ No Privacy Policy Link
New Jersey	Main Portal: http://www.state.nj.us/index.html Privacy Policy: http://www.state.nj.us/privacy.html
New Mexico	Main Portal: http://www.state.nm.us/ No Privacy Policy Link
New York	Main Portal: http://www.state.ny.us/ No Privacy Policy Link
North Carolina	Main Portal: http://www.ncgov.com/html/basic/index.html Privacy Policy: http://www.ncgov.com/asp/subpages/privacy_policy.asp
North Dakota	Main Portal: http://discovernd.com/ Privacy Policy: http://discovernd.com/privacy.html
Ohio	Main Portal: http://www.state.oh.us/ Privacy Policy: http://www.state.oh.us/ohio/privacy.htm
Oklahoma	Main Portal: http://www.state.ok.us/ No Privacy Policy Link
Oregon	Main Portal: http://www.state.or.us/ No Privacy Policy Link
Pennsylvania	Main Portal: http://www.state.pa.us/ Privacy Policy: http://www/state.pa.us/PAPower/pages/privacy.asp
Rhode Island	Main Portal: http://www.state.ri.us/ No Privacy Policy Link
South Carolina	Main Portal: http://www.state.sc.us/ No Privacy Policy Link
South Dakota	Main Portal: http://www.state.sd.us/ No Privacy Policy Link
Tennessee	Main Portal: http://www.state.tn.us/ Privacy Policy: http://www.state.tn.us/privacy.html

Texas	Main Portal: http://www.state.tx.us/ Privacy Policyhttp://www.state.tx.us/Siteinfo/privpol.html
Utah	Main Page: http://www.state.ut.us/ Privacy Policy: http://www.state.ut.us/privacy.html
Vermont	Main Page: http://www.state.vt.us/ No Privacy Policy Link
Virginia	Main Page: http://www.state.va.us/ Privacy Policy: http://www.vipnet.org/vipnet/privacy.html
Washington	Main Page: http://access.wa.gov/ Privacy Policy: http://access.wa.gov/siteinfo/pdpnotice.asp
West Virginia	Main Page: http://www.state.wv.us/ No Privacy Policy Link
Wisconsin	Main Page: http://www.state.wi.us/ No Privacy Policy Link
Wyoming	Main Page: http://www.state.wy.us/ No Privacy Policy Link
Puerto Rico	Main Page: http://fortaleza.govpr.org/ No Privacy Policy Link
US Virgin Islands	Main Page: http://www.gov.vi/ No Privacy Policy Link

Appendix II

Web Privacy Assessment

Topic Areas	Ratings	Score
ACCESSIBILITY		
Does the home page contain any Priority 1 errors? (Test at www.cast.org/bobby	Y=0 N=15	
Do image files have Alt tags with sufficient information describing the image or a null for simple images? Note: the proper code for a null is alt= "" not alt= "null"	Y=10 N=0	
Does the site provide information in accessible formats? (If all pages/documents are accessible, the site gets all 7 points)		
Are pages/documents posted in an accessible format (e.g., html)?	Y=5 N=0	
Are only image files (e.g., pdf documents) of pages/documents available?	Y=0 N=1	
Is a link for a free associated reader and instructions provided for the document image version?	Y=1 N=0	
Does the site meet the definition of a generally accessible Internet site?		
Do any pages use scrolling text?	Y=0 N=5	
Do any pages use Flash or require special plug-ins?	Y=0 N=5	
Do pages use very small text or special colors to display information?	Y=0 N=5	
Is the Web site accessible using generally available browser software?		
Does the site require a specific browser (e.g., best viewed with IE or Netscape)?	Y=0 N=2	
Does the site require a specific version for general access?	Y=0 N=1	
Home page Load Time – No Score, Just Write Down Time		
Accessibility Total (Total points possible = 50)		
PRIVACY		
Is a privacy policy published by the organization and a link provided from the home page?	Y=20 N=0	
Does the policy address the use of server logs?	Y=1 N=0	
Does the policy address information collected by other technologies or processes?	Y=3 N=0	
Does the site set a cookie to view the home page?	Y=0 N=3	
Does the site set a cookie to view the privacy policy?	Y=0 N=3	
Does the site use a Web Bug, "clear GIF," on the home page or privacy policy page?	Y=0 N=5	
Does the policy address information collected via email and Web-based forms?	Y=5 N=0	
Does every Web-based form post a link to the privacy policy?	Y=5 N=0	
Does every form that requires a citizen to enter the following information protect that information by encrypting the data via an SSL session or equivalent technology? (A) Both the individual's name and other personal information, such as an SSN; or (B) Transaction payment information; or (C) An individual's identification code and password.	Y=5 N=0	
Privacy Total (Total points possible = 50)		
Total Points		

NECCC Privacy 2000 Workgroup

Alden Schacher, Dunn & Bradstreet
Amy Moran, Wisconsin
Basil Nikas, eProcurenet
Bill Kilmartin, AMS
Brandon W. Lenoir, NECCC
Cathilea Robinett, Center for Digital Government
Cheryl Traina, AMS
CJ Brandt, Texas
Dannielle M. Germain, ITAA
Darby Patterson, Center for Digital Government
Darren Seward, IntraForce
Denise Lea, Louisiana
Dick McDonald, Louisiana
Eric Seabrook, Ohio
Ernest Almonte, Road Island
Glen Ducote, Louisiana
Jennifer Pike, NCSL
Jerry Johnson, Texas
John Ryan, CSBS
John_Gray, AMS
Jon Allison, Egovnet
Julie F. Hedlund, NACHA
Kara LaPierre, NIC
Kathryn Wilson, Maryland
Marc Hiller, New York
Mark Sutton, Kentucky
Marshall High, Idaho
Meghan Cotter, AMS
Michael L. Pinkerton, IGAPP
Nikki Trella, Maryland
Pamela Fredericks, Unisys
Rex McDonald, Louisiana
Robert Smith, Wolfenet
Robert Unger, NACHA
Sol Bermann, Ohio Supercomputer Center
Stephen Lyon, IBM
Susan Capstack, AMS

©Copyright 2000, NECCC All Rights Reserved
Reproduction of this document is encouraged with proper reference to NECCC.