Global Information Assurance Certification Paper

Brian K. Markert
GSEC Practical Assignment
Version 1.2e

Comparison of Three Online Privacy Seal Programs

The purpose of this practical is to provide evidence as to why companies should be concerned with consumer privacy and to compare three organizations' third-party assurance privacy certification programs. The three organizations that will be compared are TRUSTe, BBBOnLine and WebTrust.

Why should companies be concerned with privacy?

Companies should be concerned with privacy because consumers are concerned with privacy. During a hearing before the U.S. Senate Committee on Commerce, Science and Transportation regarding information privacy, Marc Rotenberg, Executive Director of the Electronic Privacy Information Center (EPIC) provided that following information (http://www.epic.org/privacy/internet/testimony_0701.html):

- According to Forrester Research, 90% of Americans want the ability to control the collection and use of their data.
- According to Businessweek, three times as many Americans believe the government should pass laws now to safeguard online privacy as those who believe self-regulation is sufficient.
- According to the Pew Internet and American Life Project, more than 90% of Internet users thought companies should be punished when they violate their own privacy policies.
- Also according to the Pew survey, 86% of Internet users favor opt-in privacy policies.
- In a recent Gallup Poll, 66% of email users said that the federal government should pass laws to protect citizens' privacy online. Most remarkable is that the Gallup organization found that support for legislation increased as the level of experience increased.

Another reason that companies should be concerned with privacy is that the government is reacting to consumers' concerns by passing privacy related legislation (e.g. GLBA and HIPAA) and by proposing many more pieces of privacy related legislation. Keith P. Enright, Esq. provided the following information during the Online Privacy Conference held in Chicago during July 2001:

- More than 5,000 consumer privacy bills were introduced in state legislatures in 2000
- 39 states enacted one or more consumer privacy laws
- Already in 2001, 6,918 consumer privacy bills have been introduced.

Four examples of privacy legislation that have been recently introduced by the federal

government are (http://thomas.loc.gov/home/thomas.html):

Bill Number: H.RES.159
Bill Title: Expressing the sense of the House of Representatives that machine-readable privacy policies and the Platform for Privacy Preferences Project specification, commonly known as the P3P specification, are important tools in protecting the privacy of Internet users, and for other purposes.
Bill Summary: Expresses the sense of the House of Representatives that machine-readable privacy policies and the Platform for Privacy Preferences Project specification, commonly known as the P3P specification, are important tools in protecting the privacy of Internet users. Calls for: (1) commercial and nonprofit web site operators, Members of Congress and their offices, and executive departments and agencies to deploy P3P-compliant privacy policies on their web sites; (2) legislation relating to online privacy to consider such specification; (3) the education of Internet users concerning such specification; and (4) commercial software developers to fully implement such specification.
Other Information: 6/7/2001--Introduced. Latest Major Action: 6/18/2001 Referred to House subcommittee.

Bill Number: S.450
Bill Titles: (Short Title) Financial Institution Privacy Protection Act of 2001. (Official Title) A bill to amend the Gramm-Leach-Bliley Act to provide for enhanced protection of nonpublic personal information, including health information, and for other purposes
Bill Summary: Financial Institution Privacy Protection Act of 2001 - Amends the Gramm-Leach-Bliley Act to condition financial institution disclosure of consumer nonpublic personal health information upon the consumer's affirmative consent in writing.
Replaces the opt out requirements governing such a disclosure with a prohibition against denial of a financial service or product to any consumer based upon the consumer's refusal to grant consent to nonpublic personal information disclosure.
Mandates that each financial institution designate a privacy compliance officer to ensure compliance with privacy requirements. Sets forth civil penalties for noncompliance.
Other Information: 3/1/2001--Introduced. Latest Major Action: 3/1/2001 Referred to Senate committee.

Bill Number: H.R.237
Bill Titles: (Short Title) Consumer Internet Privacy Enhancement Act. (Official Title) To protect the privacy of consumers who use the Internet.
Bill Summary: Consumer Internet Privacy Enhancement Act - Declares it unlawful for a commercial website operator to collect personally identifiable information online from a website user unless the operator provides both notice and opportunity for such user to limit its use and disclosure.
Allocates enforcement authority among designated Federal agencies and the Federal Trade Commission (FTC). Establishes a civil penalty for violations. Permits similar civil actions by the States.
Directs the FTC to contract with the National Research Council of the National Academy of Sciences for a study of online privacy and response tools and strategies.
Other Information: 1/20/2001--Introduced. Latest Major Action: 2/14/2001 Referred to House subcommittee.

Bill Number: H.R.112
Bill Titles: (Short Title) Electronic Privacy Protection Act. (Official Title) To prohibit the making, importation, exportation, distribution, sale, offer for sale, installation, or use of an information collection device without proper labeling or notice and consent.
Bill Summary: Electronic Privacy Protection Act - Makes it unlawful for any person to knowingly: (1) make, import, export, or sell an information collection device for a computer unless it has a label disclosing to the computer's primary user or to another operator who is not a primary user that it may transmit from the computer information identifiable to it; (2) install an information collection device on a computer that is not under general management and control of such person, unless such person has given notice of such installation to the computer's primary user and obtained the user's consent to such installation; or (3) use an information collection device to transmit from a computer that is not under general management and control of such person any information identifiable to such computer to a primary user or to an operator who is not a primary user, unless such person has given notice that the device may transmit such information to the primary user and obtained the user's consent to such transmission.

Sets forth civil penalties for violations of this Act.
Other Information: 1/3/2001--Introduced. Latest Major Action: 1/3/2001 Referred to House committee.

What do third-party assurance privacy certification programs offer?

A cornerstone of the TRUSTe, BBBOnLine and WebTrust privacy programs is their branded online seal, or "trustmark." The seals are displayed by websites that adhere to these organizations' established privacy requirements and agree to comply with oversight and consumer dispute resolution processes. A displayed trustmark signifies to online users that the website will openly share, at a minimum, what personal information is being gathered, how it will be used, with whom it will be shared and whether the user has an option to control its dissemination. Based on such disclosure, users can make informed decisions about whether or not to release their personally identifiable information to the website.

Organization Backgrounds

TRUSTe (http://www.truste.com/about/truste/index.html) - TRUSTe is an independent, non-profit privacy organization whose mission is to build users' trust and confidence on the Internet and, in doing so, accelerate growth of the Internet industry. TRUSTe was founded by the Electronic Frontier Foundation (EFF) and the CommerceNet Consortium. Its privacy seal program was launched during June 1997. TRUSTe's Board consists of 12 members, many of whom work for some of the most well known companies in the world including:

• Roger Cochetti	Chief Policy Officer	VeriSign
• David Hoffman	General Counsel	Intel Corporation
• Jill Lesser	SVP Domestic Public Policy	AOL Time Warner, Inc.
• Richard Purcell	Chief Privacy Officer	Microsoft Corporation

Following is a sample of TRUSTe's privacy seal: 

BBBOnLine (http://www.bbbonline.org/about/index.asp) - BBBOnLine is a wholly owned subsidiary of the Council of Better Business Bureaus. Its mission is to promote trust and confidence on the Internet through the BBBOnLine Reliability and Privacy Seal Programs. Per information provided by Gary Laden, Director of the BBBOnLine Privacy Program, during the Online Privacy Conference held in Chicago during July 2001, the privacy program was launched during March 1999. The following companies have provided leadership and financial support to BBBOnLine. Each of them has a representative on the Board of Directors:

American Online	Ameritech	AT&T Corp
Bank of America	Dun & Bradstreet	Eastman Kodak Co.
Hewlett-Packard Company	IBM Corporation	Intel Corporation
Microsoft Corporation	The Proctor & Gamble Co.	Reed Elsevier, Inc.
Road Runner	Sony Electronics	US West
Verizon	Visa	Xerox Corporation

Following is a sample of BBBOnLine's privacy seal: 

WebTrust – According to Ron Halse, American Institute of Certified Accountants (AICPA), WebTrust is a professional service developed by the AICPA and its counterpart in Canada. The professional service was launched in 1998. However, the on-line privacy standards were first available in a stand-alone format during the fall of 2000. The AICPA licenses the service to CPA firms and their equivalent, as well as to foreign institutes that, in turn, license to their members. The organizations that provide the professional service include the Big 5 and other international accounting and advisory firms, down to small firms in the US, Canada, and elsewhere.

Following is a sample of WebTrust's privacy seal: 

Organization background comparison
All three of the programs are relatively new, with the oldest being TRUSTe (June 1997). TRUSTe and BBBOnLine are similar in that they are both nonprofit organizations. WebTrust, on the other hand, is a product developed by the AICPA for use by its members. Its members are for-profit entities.

How does a company obtain each of the privacy seals?
TRUSTe (http://www.truste.com/programs/pub_how_join.html) - The following steps are required to join TRUSTe's privacy seal program:

1) Create a privacy statement – If a website already has a privacy statement consistent with the information contained in TRUSTe's self-assessment document, it may be submitted with the application packet. If no privacy statement exists, TRUSTe provides an online Privacy Resource Guide (http://www.truste.com/bus/pub_resourceguide.html) for assistance. The Privacy Resource Guide provides the framework for creating a privacy statement, which should be tailored to reflect the specific privacy practices of the requesting company's website.

2) Complete the required paperwork – The requesting company should first read the license agreement. In signing the license agreement, the requesting company agrees to follow the established privacy principles outlined by TRUSTe and comply with their oversight and resolution process. An important element of the license agreement is the self-assessment form (http://www.truste.com/programs/pub_how_join.html - step2). The self-assessment form asks for a detailed account of the requesting company's internal privacy and security practices.

3) The application is processed - The application processing department contacts a requesting company within 10 –15 business days after receipt of the application. Once TRUSTe has verified that all of the required information has been provided, an account executive manager contacts the requesting company within 45-60 days. The account executive manager will conduct the certification and review process via a phone conference.

BBBOnLine (http://www.bbbonline.org/privacy/apply.asp) - The following steps are required to join BBBOnLine's privacy seal program:

1) The requesting company must first complete the Business Application and pay the Application and Annual Assessment Evaluation fees. The fees must be submitted with the application. Once an application has been submitted, an e-mail will be received by the requesting company directing it to complete the Compliance Assessment Questionnaire.

2) Complete the Compliance Assessment Questionnaire (http://www.bbbonline.org/privacy/assess.pdf) – The questionnaire is the basis for determining a company's eligibility for the privacy seal program. The questionnaire will be assigned to a Compliance Analyst for review. Once BBB*OnLine* has reviewed a company's website and has notified the company of any outstanding issues, the company is required to respond within 60 days. After 60 days without a response, all applications are considered inactive and companies will need to submit a new application and questionnaire, including additional application and evaluation fees.

3) Sign and submit the Participant (License) Agreement and return it to BBBOnLine (http://www.bbbonline.org/privacy/license.pdf).

WebTrust (http://www.cpawebtrust.org/privacy_fin.htm) - The following steps are required to join WebTrust's privacy seal program:

1) Contact a specially trained, licensed WebTrust provider. A company can find a WebTrust provider by asking its CPA, Chartered Accountant, or equivalent whether he or she offers WebTrust or by contacting the American Institute of Certified Public Accountants or similar institute in the appropriate country and requesting a list of WebTrust providers.

2) Meet the WebTrust's Principles for Privacy as measured by the WebTrust Criteria.

3) Obtain an unqualified report from the WebTrust provider.

Obtaining the privacy seal process comparison

The TRUSTe and BBBOnLine programs are somewhat similar. Each of these programs relies heavily on a self-assessment process and a high-level review of the self-assessment by a TRUSTe or BBBOnLine analyst. WebTrust's program, on the other hand, includes a much more detailed review of an organization's privacy practices and relies less on an organization's self-assessment.

How are consumer privacy complaints handled?

TRUSTe (http://www.truste.com/users/compliance_doc.htm) - TRUSTe's privacy seal program provides online third party dispute resolution for complaints reported by consumers regarding a licensed TRUSTe website. This service is called the WatchDog Dispute Resolution process. It is available at no cost to any consumer who files a privacy-related complaint online. The WatchDog Dispute Resolution process allows TRUSTe to initiate a negotiation between the individual and the company. At no point is the individual's right to legal recourse affected. While the outcome is not binding on the individual, the company must comply with TRUSTe's final determination or face removal from the TRUSTe program, breach of contract legal proceeding, and/or referral to the appropriate governing body.

BBBOnLine (http://www.bbbonline.org/consumer/procedure.asp) - BBBOnLine uses its Privacy Policy

Review Service (PPRS) to process consumer complaints. The PPRS is responsible in the dispute resolution process for determining the eligibility of a complaint and evaluating, investigating, analyzing and making a decision on the merits of an eligible complaint. The PPRS will make a final determination as to whether a complaint is eligible and, if so, continue with its dispute resolution process
Under the PPRS process, before filing a privacy complaint form, the complainant is required to review the eligibility criteria to verify that the complaint is a privacy matter relating specifically to the website (http://www.bbbonline.org/consumer/submit.asp). Next, the complainant should contact the website owner directly to make a good faith effort to resolve the complaint through direct contact. Then, if the website owner does not satisfactorily resolve the complaint; the PPRS can be notified for help.

WebTrust (http://www.cpawebtrust.org/privacy_fin.htm) - The WebTrust privacy program encourages the use of the twelve principles that form the basis of the arbitration process developed by the National Arbitration Forum (NAF). NAF is an organization that is based in the U.S. and has developed an arbitration process that is widely used. It is the model adopted by WebTrust regardless of whether NAF or another organization is selected for the arbitration process.

Complaints can be initiated with the NAF via the Internet, telephone or the regular mail. It costs $49 for claims less than $1,000 and between $49 - $150 for claims greater than $1,000. The losing party pays the costs. Most disputes are typically resolved within 45 – 60 days. If one of the parties is not satisfied with NAF's decision, the party can still go to court.

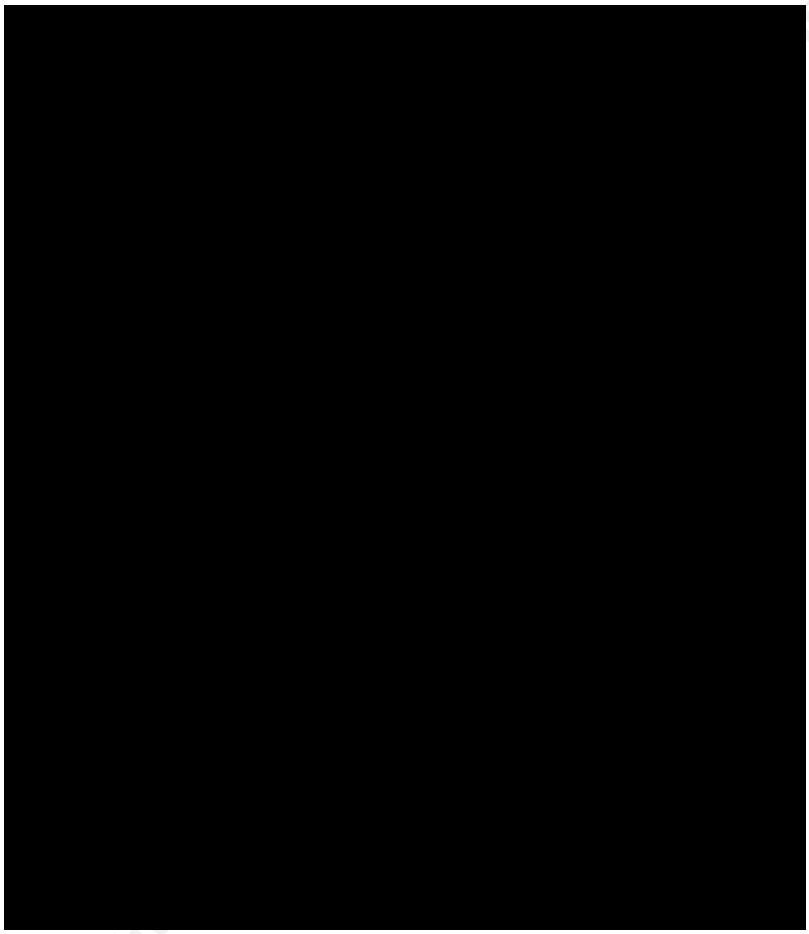
Consumer privacy complaint process comparison
The consumer privacy complaint process for both TRUSTe and BBBOnLine are similar. They are both free and are handled by departments within the TRUSTe and BBBOnLine organizations. Consumer privacy complaints for WebTrust licensed websites are handled through an organization outside of the WebTrust privacy seal program. Also, there is a nominal fee involved.

What are the vendor costs?
TRUSTe (http://www.truste.com/bus/pub_fees.html) - The cost of acquiring a license to display the TRUSTe privacy seal is dependent upon a company's overall revenue. In cases of subsidiaries, the measure to use is the overall annual revenue of the parent company. The following table displays the annual fee by amount of company revenue.

Company's Annual Revenue	Annual Fee
$0 - $1 million	$299
$1 - $5 million	$399
$5 - $10 million	$599
$10 - $25 million	$1,999
$25 - $50 million	$2,999
$50 - $75 million	$3,999
$75 million and over	$6,999

BBBOnLine (http://www.bbbonline.org/privacy/price.asp) - All BBBOnLine privacy seal program

applicants pay a one-time $75.00 application fee in addition to the annual assessment evaluation fee. The application fee is non-refundable. If based on a preliminary review of the application a company does not meet the threshold standards, an assessment evaluation will not be conducted and the assessment evaluation fee will be refunded. If a company meets the threshold standards, an assessment evaluation will be conducted and the assessment evaluation fee is non-refundable. The following table displays the annual fee by amount of company revenue.



WebTrust (http://www.webtrust.org/onlstart.htm) - Estimated costs must be obtained from a specially trained and licensed WebTrust provider. WebTrust providers are typically CPA's, Chartered Accountants or an equivalent. There are two main costs. One cost is the fee of the WebTrust provider who examines a company's electronic commerce. This fee reflects the work required to assure a company and its customers that all applicable WebTrust standards are met. The other cost is an annual fee for the digital certificate that authenticates the WebTrust seal and proves that a company has earned the WebTrust mark. These costs are not published and are specific to the company for which the services are provided.

Vendor cost comparison

The TRUSTe and BBBOnLine cost structures are similar in that they are both based upon companies' total revenue. Also, their maximum fees are comparable as TRUSTe tops out at $6,999 per year and BBBOnLine tops out at $6,000 per year. However, TRUSTe tops out at a

much lower company revenue ($75 million) than BBBOnLine ($2 billion). Since WebTrust does not have a set cost structure and does not publish costs, it is difficult to compare the costs of obtaining its privacy seal versus TRUSTe and BBBOnLine. However, it is assumed that the costs of the WebTrust privacy program are significantly higher due to the extensive review performed under the program guidelines as compared to the relatively high-level review performed under the TRUSTe and BBBOnLine program guidelines.

Who are some of the organizations' customers?

TRUSTe (http://www.truste.com/users/users_lookup.html) - As of 7-29-01, per a manual count of the licensed websites listed on TRUSTe's website, there were 1,597 websites participating in the privacy program (however, other information provided by TRUSTe indicates that there are more than 1,597 websites licensed to use TRUSTe's privacy seal). A small sampling of the participant list and the websites at which the TRUSTe seal is displayed follows:

ABC http://disney.go.com/corporate/legal/wdig_privacy.html
IBM http://www.ibm.com/privacy/us/
State Farm Insurance Company http://www.statefarm.com/about/privacy.htm

BBBOnLine (http://www.bbbonline.org/) - As of 7-29-01, there were 852 websites participating in the privacy program. A small sampling of the participant list and the websites at which the BBBOnLine seal is displayed follows:

Dell Computer http://www.dell.com/us/en/gen/misc/policy_000_policy.htm
Kodak http://www.kodak.com/US/en/corp/privacy/index.shtml
Xerox
http://www.xerox.com/go/xrx/template/009.jsp?view=Privacy&Xcntry=USA&Xlang=en_US&Xseg=corp

WebTrust (http://www.webtrust.org/abtseals.htm) - As of 7-29-01, there were 25 websites participating in the WebTrust program. A small sampling of the privacy program participant list and the websites at which the WebTrust seal is displayed follows:

American Institute of Certified Public Accountants http://www.aicpa.org/index.htm
HD Vest Financial Services http://www.hdvest.com/
Portera http://www.portera.com/

Customer comparison

TRUSTe, which is the oldest of the three privacy seal programs, has by far the most licensed websites, almost doubling the volume of BBBOnLine. WebTrust's volume, which is the newest of the three privacy seal programs, does not yet compare to the volume of either TRUSTe or BBBOnLine. However, according to Websense (http://www.websense.com/products/about/faqs/index.cfm - how), there are at least 2.5 million existing websites. Considering only about 2,500 of these websites are licensed by at least one of the three organizations', there is much room for expansion in the privacy seal program market. Another indication of room for expansion in this market is that some organizations are obtaining more than one privacy seal. Three examples of

companies that have acquired both the TRUSTe and BBBOnLine privacy seals are:

Amica Mutual Insurance Company http://www.amica.com
The New York Times http://www.nytimes.com/info/help/privacy.html
Intel Corporation http://www.intel.com/sites/corporate/privacy.htm?iid=intelhome+privacy&

One example of a company that has acquired both the WebTrust and BBBOnLine online privacy seals is:

HD Vest Financial Services http://www.hdvest.com/

Privacy seal program caveats

Patrick F. Sullivan, Ph.D provided the following information during the Online Privacy Conference held in Chicago during July 2001 regarding privacy seal programs:

> "Seal programs will provide applicants with review criteria based on the general principles and disclosure requirements of the program. These facilitate documenting practices that support disclosures but involve no substantive testing of controls by the seal program, and do not result in an opinion on the compliance of the organization".

This appears to be true of the privacy seal programs offered by TRUSTe and BBBOnLine. However, qualifying for the WebTrust privacy seal does involve substantive testing and an opinion is provided.

Also per Patrick F. Sullivan, "seal program standards do not yet incorporate content required by regulations such as GLBA and HIPAA".

Conclusion

Two of the three organizations' privacy seal programs (TRUSTe and BBBOnLine) are very similar including:

- They are both non-profit organizations
- The process to obtain their privacy seals relies heavily on self-assessments
- Consumer complaints are handled within the organization and is free
- Their cost structures for obtaining a privacy seal are both based upon total revenue and total potential vendor costs are similar ($6,999 for TRUSTe versus $6,000 for BBBOnLine).

WebTrust, on the other hand:

- Is obtained through WebTrust providers which are for-profit entities (typically, CPA's)
- Relies heavily on a thorough examination by the WebTrust provider
- Handles consumer complaints through an organization external to the WebTrust program
- Does not publish its cost structure since it varies from customer to customer depending on the specific arrangement between the WebTrust provider and the requesting company.

In summary, it appears that TRUSTe and BBBOnLine offer a minimal baseline of assurance that consumers' personally identifiable information is handled appropriately. Likewise, their privacy

seals can be obtained at a minimal cost. WebTrust, however, offers a much greater amount of assurance that consumers' personally identifiable information is handled appropriately, but at what is assumed to be a much greater cost.

According to information provided by TRUSTe during the Online Privacy Conference held in Chicago during July 2001, 55 % of web users indicated that the presence of the TRUSTe seal increased trust in a site. How important consumers perceive the protection of their personally identifiable information to be will determine to what extent the privacy seal program market grows and which type of privacy seal program flourishes.

Internet References:

http://thomas.loc.gov/home/thomas.html
http://www.epic.org/privacy/internet/testimony_0701.html
http://www.websense.com/products/about/faqs/index.cfm - how

TRUSTe Internet Sites Referenced

http://www.truste.com/about/truste/index.html
http://www.truste.com/programs/pub_how_join.html
http://www.truste.com/bus/pub_resourceguide.html
http://www.truste.com/programs/pub_how_join.html - step2
http://www.truste.com/users/compliance_doc.htm
http://www.truste.com/bus/pub_fees.html
http://www.truste.com/users/users_lookup.html

BBBOnLine Internet Sites Referenced

http://www.bbbonline.org/about/index.asp
http://www.bbbonline.org/privacy/apply.asp
http://www.bbbonline.org/privacy/assess.pdf
http://www.bbbonline.org/privacy/license.pdf
http://www.bbbonline.org/consumer/procedure.asp
http://www.bbbonline.org/consumer/submit.asp
http://www.bbbonline.org/privacy/price.asp
http://www.bbbonline.org/

WebTrust Internet Sites Referenced

http://www.cpawebtrust.org/privacy_fin.htm
http://www.cpawebtrust.org/privacy_fin.htm
http://www.webtrust.org/onlstart.htm
http://www.webtrust.org/abtseals.htm

Miscellaneous Internet Sites Referenced (sites that display privacy seals)

http://disney.go.com/corporate/legal/wdig_privacy.html
http://www.ibm.com/privacy/us/
http://www.statefarm.com/about/privacy.htm
http://www.dell.com/us/en/gen/misc/policy_000_policy.htm
http://www.kodak.com/US/en/corp/privacy/index.shtml
http://www.xerox.com/go/xrx/template/009.jsp?view=Privacy&Xcntry=USA&Xlang=en_US&Xseg=corp
http://www.aicpa.org/index.htm

http://www.hdvest.com/
http://www.portera.com/
http://www.amica.com
http://www.nytimes.com/info/help/privacy.html
http://www.intel.com/sites/corporate/privacy.htm?iid=intelhome+privacy&
http://www.hdvest.com/

Other References:

Keith P. Enright, Esq., "Access Requirements Facing Business"
The Online Privacy Conference (July 17-18, 2001)

Patrick F. Sullivan, Ph.D, "Auditing the Privacy Compliance of Web Sites: Are My Lips Really Sealed?"
The Online Privacy Conference (July 17-18, 2001)

Becky Richards, "TRUSTe Privacy Assurance"
The Online Privacy Conference (July 17-18, 2001)