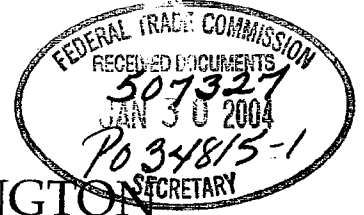




Christine O. Gregoire

ATTORNEY GENERAL OF WASHINGTON

1125 Washington Street SE • PO Box 40100 • Olympia WA 98504-0100



January 16, 2004

Federal Trade Commission
Office of the Secretary, Room 159-H
Pennsylvania Avenue NW
Washington, DC 20580

RE: Alternative Forms of Privacy Notices, Project No. PO34815

I am writing to comment on the proposed rule to improve privacy notices financial institutions provide to consumers under the Gramm-Leach-Bliley Act. I applaud your efforts to improve the readability and clarity of privacy notices.

The Washington State Attorney General's Office has been active on consumer privacy issues since 1999. That year my Office led a task force on consumer privacy that included consumer and privacy advocates, business leaders, legislators and concerned others. The task force produced a report that highlighted growing consumer concerns over how their personal information was being used by businesses. The report also noted the importance of balancing consumer concerns with the legitimate needs of business to market their products.

Since that time, the Attorney General's Office has responded to the privacy issue by sponsoring and supporting legislative solutions and by taking enforcement actions where appropriate. In addition, the Attorney General's Office in conjunction with the University of Washington's Shidler Center for Law Commerce and Technology released a report in 2002 containing suggested "best practices" for protecting personal information collected by businesses. The report analyzed the then state of federal and state law, self-regulatory industry practices, and consumer concerns. It all also included principles to guide businesses that will increase consumer confidence.

I have enclosed the best practices portion of the report as the Washington State Attorney General's Office public input submission. The entire report can be downloaded from our website at www.atg.wa.gov. If we can be of further assistance please feel free to contact my office. Please contact Special Assistant for Policy and Government Relations, Brian Smith, at 360-664-4953 or by email at BrianS1@atg.wa.gov.

Sincerely,

A handwritten signature in cursive script that reads "Christine Gregoire".

CHRISTINE O. GREGOIRE
Attorney General

Enclosure



information, they won't leave anything to question, and won't be targeted by regulators. Some decide to disclose nothing, operating on the theory that if they make no assurances about protecting the privacy of consumers' private information, they won't be accused later of making misrepresentations, should information inadvertently slip out, or should their privacy policy change.

Neither over-disclosure nor non-disclosure serves businesses or consumers well. If a business chooses overwhelming disclosure, as was seen in the recent disclosure and opt-out program mandated by the Graham-Leach-Bliley Act, consumers simply do not read the information. Thus, the right to opt out becomes meaningless. Likewise, if the consumer is given no disclosure, and no right to exercise a choice about the use or sharing of personal information, he or she has no knowledge, and no control over personal information.

However, a middle ground exists. While businesses, regulators, and consumers may disagree over the exact details of what should be included in a privacy policy, there is an area where agreement can be reached at least in terms of how businesses can provide meaningful disclosure. When a business chooses to afford privacy protections to consumers, it should describe those protections in a way that consumers can understand.

The balance of this report discusses a menu of "best practices." It emphasizes the need for meaningful disclosure. The report suggests a two-step approach for privacy policies--a one-page summary for consumers highlighting the privacy policy and a more comprehensive explanation of the policy attached or hyperlinked to the one-page summary. It discusses the importance of creating a policy that most Americans are able to read and understand. It does not mandate that the most protective policy be adopted, but gives businesses a number of options based on their own decisions about the necessary level of protection.

The "best practices" suggested in the balance of this report are applicable to both the online and the "brick and mortar" world.

A. PRIVACY POLICY GUIDELINES – GENERAL OVERVIEW¹⁰¹

Introduction:

These guidelines are provided as an example for businesses to utilize when developing their own privacy policies. Each business should take into consideration the needs of their own business practices vis-à-vis their customers' preferences when developing a privacy policy. Business models vary, as do data use and retention practices. The differences in business

¹⁰¹ The skeleton of this guideline was adopted from the Better Business Bureau Online Privacy Seal Program Requirements. See www.bbbonline.org

structure and size make a one-size-fits all policy impossible. Accordingly, the following recommendations are made with the knowledge that they may need to be adapted to fit a particular business' constraints:

- a. The privacy notice should be easy to read, follow, and understand.
- b. The privacy notice should be easily located and be clearly and conspicuously presented on all the home pages of the firms' web sites, services, affiliated links¹⁰² or other Internet mediums at which the firm collects personally identifiable information, including electronic mail addresses.
- c. Notices which are given offline should be likewise clear and conspicuous, and provided to the customer at a meaningful time in an appropriate medium.
- d. The privacy notice should be written in language and terms that are easily understood by the average individual. The readability factor should comport to the reading level of the average adult based on the Flesch reading scale.¹⁰³
- e. The privacy notice should be displayed in a simple text format with minimal graphics.
- f. The privacy notice should contain all required disclosures in a single document in a one-page summary linked to the policy itself either through a direct reference or a hyperlink.
- g. If the business is engaged European Union-United States data transfers, then the privacy notice should comply with the safe harbor privacy principles set forth by the United States

¹⁰² "Affiliated links" refers to links owned and/or operated by "affiliates." "Affiliates" are generally businesses that have common ownership relationships with other business entities. The most common example is a parent and subsidiary relationship. The Gramm-Leach-Bliley Act defines "affiliates" as any company that controls, is controlled by, or is under common control with another company.

¹⁰³ The Flesch Reading Ease Scale measures readability as follows:

| | | |
|-----|------------------------------|---|
| 100 | Very easy to read. | Average sentence length is 12 words or less. No words of more than two syllables. |
| 65 | Plain English. | Average sentence length is 15 to 20 words. Average word has two syllables. |
| 0 | Extremely difficult to read. | Average sentence length is 37 words. Average word has more than two syllables. |

The higher the score, the easier the text is to understand. By the very nature of technical subject matter, the Flesch score is usually relatively low for technical documentation. The approach to calculating the Flesch score is as follows: (1) Calculate the average sentence length, L.; (2) Calculate the average number of syllables per word, N.; (3) Calculate score (between 0-100%). See generally [http://www.mang.canterbury.ac.nz/courseinfo/Academic Writing/Flesch.htm](http://www.mang.canterbury.ac.nz/courseinfo/Academic%20Writing/Flesch.htm).

Department of Commerce. These principles were developed in compliance with the European Union's Directive on Data Protection.^{104 105}

- h. The privacy notice should build upon the core principles espoused by the Federal Trade Commission, e.g., notice, choice, access, and enforcement.¹⁰⁶
- i. The privacy policy should refer to existing law applicable to the particular business.¹⁰⁷

2. Privacy Notice Content

a. Notice

1. The privacy notice should be clearly and conspicuously written and presented.
2. The privacy notice should be easy to find, not buried on the page in an obscure spot, and not hidden in fine print.
3. The privacy notice should specify the various types and categories of personally identifiable information¹⁰⁸ actually collected, or any information that will be collected in the future. In addition, the organization should notify individuals regarding purposes for which they collect and use such information.¹⁰⁹

¹⁰⁴ See www.export.gov/safeharbor/SHPRINCIPLESFINAL.htm

¹⁰⁵ The U.S. Department of Commerce in consultation with the European Commission developed a safe harbor framework. The safe harbor--approved by the EU this year--is an important way for U.S. companies to avoid experiencing interruptions in their business dealings with the EU or facing prosecution by European authorities under European privacy laws. See www.export.gov/safeharbor/sh_overview.html

¹⁰⁶ See Federal Trade Commission May 2000, A Report to Congress, Privacy Online: Fair Information practices In The Electronic Marketplace. (The core privacy principles espoused by the FTC are Notice, Consent, Access and Correction, Security, Enforcement, and no State preemption).

¹⁰⁷ These guideline provisions are to cover sites not already covered by the following regulatory measures. Congress has enacted privacy regulatory measures for the following areas: Government (Privacy Act of 1974, 5 USC § 552a(1994)); The cable industry (Cable Communications Policy Act of 1984, Pub.L.No. 98-549, 98 Stat. 2779 (codified as amended in scattered sections of 47 U.S.C.)); Video rental industry (Video Privacy Protection Act of 1988, 18 U.S.C. §§ 2710-2711 (1988)); Banking and Finance (Right to Financial Privacy Act of 1978, 12 U.S.C. §§ 3401-3422 (1978)); Gramm-Leach-Bliley Act of 1999, 15 U.S.C. §6801, Fair Credit Reporting Act, 15 U.S.C. §601; Electronic Communications (Electronic Communications Privacy Act of 1986 (ECPA)), 18 U.S.C. §2511; Children's Online Privacy Protection Act of 1998, 15 U.S.C. §6501.

¹⁰⁸ "Personally Identifiable Information" is defined as any piece of information that relates to an identified or identifiable natural person. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifiable name, number or to other factors more specific to one's physical, physiological, mental, economic, cultural or social identity. See www.export.gov/safeharbor/sh_workbook.html

¹⁰⁹ In order to comply with the Department of Commerce safe harbor (NOTICE) principle, organizations must notify individuals about the purposes for which they collect and use information about them. They must provide information about how individuals can contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information and the choices and means the organization offers for limiting its use and disclosure. See www.export.gov/safeharbor/sh_overview.html

4. If no personally identifiable information is actually collected, or will be collected in the future, then the privacy notice should state this fact in a clear and conspicuous manner.
5. The privacy notice should disclose with whom the information is shared. In the case of online organizations, if there exist links between web sites or online services covered by the policy and non-covered web sites or online services, maintained by the online organization, the privacy notice should identify by URL (or some other identifier) the non-covered web sites or online service.
6. If information is shared with, used by, or sold to affiliates or unaffiliated third parties the notice should disclose the identity of those affiliates or unaffiliated third parties. The affiliates or unaffiliated third parties should be bound by the covered firm's privacy policy.¹¹⁰
7. For each type and category of personally identifiable information actually collected or that will be collected in the future, the privacy notice should clearly and specifically disclose how that information will be subsequently used, processed, shared, or sold to any other third party business entity or entity within their own organization.
8. If the organization limits the privacy promises stated in the privacy notice to residents of one particular geographical, or other category of jurisdiction, the notice should so state in a clear and conspicuous manner. The limitations should be presented in an obvious manner and not buried in fine print, or at the bottom of the page.
9. The privacy notice should clearly explain how a consumer may access and review all their personally identifiable information that has been collected or will be collected in the future. The firm should maintain all personally identifiable information in retrievable form. If personally identifiable information is collected, and not maintained in retrievable form, the privacy notice should so disclose. In addition, the organization should provide alternative means to obtain access to the information collected and provide a mechanism to make factual corrections through another medium (i.e. hard copy corrections via the U.S. Postal Service).¹¹¹

¹¹⁰ In order to comply with the Department of Commerce safe harbor (ONWARD TRANSFER) principle, organizations that disclose information to a third party must apply the notice and choice principles. Where an organization wishes to transfer information to a third party that is acting as an agent, it may do so if it makes sure that the third party subscribes to the safe harbor principles or is subject to the Directive or another adequacy finding. As an alternative, the organization can enter into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant principle. See www.export.gov/safeharbor/sh_overview.html

¹¹¹ The term "corrections" includes, but is not limited to, amending, deleting, updating, and modifying the collected data to ensure accuracy.

10. The privacy notice should clearly explain how a consumer may make factual corrections and update all their personally identifiable information that has been collected or will be collected in the future.
11. If an organization utilizes 'cookies'¹¹² to gather any personally identifiable information and/or transaction-generated information, it should disclose this fact in a clear and conspicuous manner.¹¹³ In addition, the organization should clearly and specifically disclose how the information, retrieved by the cookie(s), will be utilized. If this information is subsequently shared and/or sold to affiliates or other third parties, it should be disclosed to the user. Moreover, the organization should clearly and explicitly explain how individuals may prevent this transfer of information, at any time, by opting-in or opting-out.
12. If the organization uses personally identifiable information for its own direct marketing, the privacy notice should explain how an individual can, at any time, opt-in or opt-out of this direct marketing.¹¹⁴
13. The privacy notice should state the organization's commitment to data security. The organization should specifically describe what measures they take to protect and safeguard the information.
14. The privacy notice should provide contact information for the organization in the instance there are questions or concerns about the organization's privacy and security policies.
15. If information submitted by individuals acting solely in a business capacity (such as a purchasing agent) is excluded from the protections of the privacy notice, the privacy notice should clearly and conspicuously disclose this fact.

¹¹² "Cookies" allow web sites to store information about one's visit to that site on their hard drive. If a user returns to the web site, cookies will read the user's hard drive to find out if they have been there before. The web site will typically use the information that they learn about the user, to market certain products and/or services to them.

¹¹³ "Transaction-Generated Information" is a term that describes information that is collected from cookies that monitor a user's browsing pattern. The information collected is highly valuable for marketers.

¹¹⁴ In order to comply with the Department of Commerce safe harbor (CHOICE) principle, organizations must give individuals the opportunity to choose (opt-out) whether their personal information will be disclosed to a third party or used for a purpose incompatible with the purpose for which it was originally collected or subsequently authorized by the individual. For sensitive information, affirmative or explicit (opt-in) choice must be given if the information is to be disclosed to a third party or used for a purpose other than its original purpose authorized subsequently by the individual. ["Sensitive" Data is information that pertains to racial or ethnic origins, political or religious beliefs, or health or sex life.] See www.export.gov/safeharbor/sh_overview.htm

16. If access to any part of the site or service is conditioned on the disclosure of personally identifiable information, the privacy notice should disclose this fact at the point of collection.
17. If information collected online is combined with data obtained from outside parties for purposes of an organization's marketing or any other affiliated or unaffiliated firm's marketing or for any other business endeavor, the privacy notice should disclose this fact in a clear and conspicuous manner.
18. If there are other organizations that reside on a firm's web site or online service and collect personally identifiable information from individuals while they remain on the web site or online service, then the privacy notice should disclose this fact in a clear and conspicuous manner. No information should be collected unless the user has an opportunity to evaluate the other organizations' privacy policies and has the opportunity to opt in or opt out of the data collection. This disclosure and opportunity should be available prior to any collection of data. The privacy notice should identify these other organizations and provide a URL (or some other form of contact information) that would allow an individual the opportunity to evaluate the privacy and security policies of these other organizations.
19. For online businesses, the privacy notice should provide a special note regarding children. Organizations should follow the legal guidelines set forth by the Children's Online Privacy Protection Act (COPPA).¹¹⁵
20. If a business has frequently changing business relationships, an effort should be made to update the privacy policy on a regular basis (e.g., quarterly) and to alert consumers to the fact that the privacy policy will be updated periodically. Large businesses may have frequently changing business relationships, which impact their ability to provide up-to-the-minute notice concerning various aspects of their privacy practices. Given this factor, such businesses should state how often they and their affiliates update their privacy policy to take into account new use of personal data as well as changes to the list of parties with whom the business shares information.

b. Shared Information

1. All firm employees, agents, contractors, or other affiliated personnel who have access to personally identifiable information should honor the organization's privacy and security

¹¹⁵ COPPA, 15 U.S.C. §§ 6501-6506. Section 6502(a) of COPPA prohibits the collection of "personal information" from children under the age of 13 by operators of web sites and on-line services that are directed to children, as well as by operators who knowingly collect personal information from children under the age of 13, in a manner that violates specific regulations promulgated by the FTC. 15 U.S.C. § 6502(a).

policies, hold such information in confidence, and not use such information for any purpose other than to carry out the services they are performing for the organization.

2. An organization should not share any personally identifiable information with any outside party or corporate affiliates when such parties may use such information for their own or subsequent parties' marketing or any other endeavor, without notifying the individual to whom the information relates. The organization should provide the individual an opportunity to opt in or opt out.
3. When the organization transfers any personally identifiable information to outside parties or corporate affiliates, the organization should have in place mechanisms to ensure that such parties are aware of the organization's privacy and security policies applicable to such data. Furthermore, such parties should take reasonable precautions to similarly protect such information.

c. Consent

1. Where an organization uses personally identifiable information for its own direct marketing, it should provide individuals with a choice concerning the direct marketing.
2. An organization should provide individuals a choice about the use of information about them that was not permitted in the privacy notice in effect at the time the information was collected or that is unrelated to the purpose for which the information was collected.
3. The organization should provide individuals with a choice regarding the transfer of information to outside parties; if corporate affiliates operate under a different privacy policy, the organization should note that some of the affiliates with whom it shares data might have different privacy policies.
4. Where the web site conditions the granting of access to some or all of its web site(s) or online service(s) based on the disclosure of personally identifiable information, the organization should inform individuals, in its privacy notice or at the point of collection, of the consequences of refusing to provide such information.

d. Access and Correction

1. An organization should have in place a reasonable process, unlimited by frequency or fee, by which factual inaccuracies in information collected and maintained in retrievable form may be corrected upon request. In addition, the process should be easily utilized by the average individual. Any corrections should be amended in a timely manner.

