California Information-Sharing Disclosures and Privacy Policy Statements

November 22, 2004

Arnold Schwarzenegger
Governor

Fred Aguiar
Secretary
State and Consumer Services Agency

Charlene Zettel
Director
Department of Consumer Affairs

Joanne McNabb
Chief
Office of Privacy Protection

www.privacy.ca.gov
866-785-9663

Contents

As Director of the California Department of Consumer Affairs, I am providing this document in fulfillment of the Office of Privacy Protection's statutory mandate to "make recommendations to organizations for privacy policies and practices that promote and protect the interests of California consumers" (Business and Professions Code section 350(c)).

In light of the dramatic increases in identity theft in recent years, all organizations are engaged in reviewing and improving their practices for handling the personal information entrusted to them. The Department's Office of Privacy Protection offers these recommendations to assist businesses and other organizations in conducting such reviews. The recommendations are not binding, but are suggestions for organizations to consider.

Providing these recommendations is part of the Department's fundamental mission of developing a fair marketplace. The Department of Consumer Affairs is here for all Californians, continuing the tradition of providing protection, education and resources to consumers, businesses and the people of this great state

Charlene Zettel
Director
California Department of Consumer Affairs

Introduction

Privacy Notice Laws

As was the case for each prior set of recommended practices issued by the Office of Privacy Protection, this set of recommendations addresses practical issues raised by new California privacy laws. The "shine the light" law, well known as SB 27, imposes specific privacy notice requirements on certain businesses that share customer personal information with others for marketing purposes.[1] This law is unique in requiring disclosure of the details of a business's sharing of customer personal information. The "shine the light" law was a response to growing consumer concern about such information sharing. This document also addresses the broader topic of privacy policy statements, including the requirements of the California Online Privacy Protection Act.[2]

Over the past three decades, an international consensus has developed regarding general guidelines for collecting and managing personal information, expressed as the Fair Information Practice Principles.[3] The United States of America, as a member of the Organisation for Economic Co-operation and Development, participated in the development of these principles and reaffirmed their viability as recently as 1998, in the *Declaration on the Protection of Privacy in Global Networks*.[4] In that work, the U.S. committed to respecting individual privacy rights as an essential component to building and retaining public confidence in a marketplace that is increasingly global and increasingly online. The Principles form the foundation of most privacy laws in the U.S. and elsewhere.

The issue of giving meaningful notice of privacy policies and practices concerns the most basic Fair Information Practice Principle: Openness. The issue has received considerable legislative attention. In developing the present recommendations, the Office of Privacy Protection considered several major laws in this area. The laws whose notice provisions we reviewed included, in addition to the California Online Privacy Protection Act, the California Financial Information Privacy Act; the federal privacy regulations and guidance on the Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act, and the Safe Harbor framework; Canada's Personal Information Protection and Electronic Documents Act; and the European Union's Data Protection Directive.[5] We note that the notice provisions of these different laws appear to be complementary. Nonetheless, meeting the requirements of several of them at once, as some companies must do, may present challenges in certain instances.

Privacy and Customer Trust

Recent research in the U.S. confirms the need for organizations to earn consumer confidence in the way they manage personal information. A national survey conducted in June 2004 by Privacy and American Business (P&AB) with Harris Interactive found that more Americans are acting on their privacy concerns today than five years ago.[6] Consumers are particularly unhappy about the unauthorized use of their personal information for marketing, whether the use is by a company with which the consumer has a business relationship or by other companies with which the information was shared. The P&AB survey found that 87 percent of consumers had asked a company to remove their name and address from marketing lists, an increase of 29 percent since 1999. An equally striking 81 percent had asked a company not to sell or give their name and address to another company, up 28 percent

since 1999. The P&AB survey also found that 65 percent of consumers online – more than 94 million people – decided not to register at a Web site because they deemed the privacy policy too complicated or unclear. Thus, an effective privacy policy statement is a critical element in winning customers online.

According to Dr. Alan Westin, a national expert on information privacy and the president of P&AB, the survey results confirm, "not just consumer resistance to what they see as intrusive marketing probes, but a clear desire to be given and to be able to exercise rational personal choices in how marketing to them is conducted by the companies those consumers already patronize."[7]

Another national study conducted in June 2004 by the Ponemon Institute (a think tank on privacy and information security policy) found that consumers gauge a company's privacy trustworthiness by three criteria. The most important factor is the company's overall reputation for product and service quality, followed by the company's limits on collection of its customers' personal information. The third factor is the use of advertisements and solicitations that respect consumer privacy.[8]

Other studies by the Ponemon Institute have found that organizations that achieve higher privacy trust ratings experience tangible positive outcomes.[9] Examples of positive outcomes include higher consumer data accuracy, higher customer participation in online activities, lower customer churn rates, and much higher product or brand loyalty. The following key activities were common among companies with high scores:

- Providing clear and concise privacy policy statements and notices, including explaining the distinction between Web and non-Web privacy practices.
- Offering customers the ability to participate in data collection and use decisions, with well defined steps for opting in or out.
- Setting limits on data sharing and providing clear information on how shared data will be used.
- Providing well defined steps for redress and for making general inquiries about privacy issues.

More companies today recognize that respect for privacy is an essential component of customer trust and that privacy statements are, as a Canadian privacy official puts it, relationship builders rather than legal disclaimers.[10] We offer these recommendations to encourage the provision of meaningful and understandable statements of a company's privacy practices. Such openness enables consumers to play their proper role in a robust free market.

Benchmark Study

In June 2004, the Ponemon Institute conducted a preliminary benchmark study on corporate preparations for California's "shine the light" law. Based on interviews with 32 mostly large companies, the study results show that some are striving to do more to track and control data sharing with direct marketers, including using data-tracking technology. A majority of the companies, however, see the requirement as a fairly simple revision to their existing privacy disclosure and notice process. The major changes being implemented included Web site redesign, printing and distributing customer information on the new law, and awareness training for customer contact personnel. Several respondents mentioned that the new requirement gave them an opportunity to build trust and confidence with customers. More information on the survey results is available from the Ponemon Institute.[11]

The Office of Privacy Protection's Recommended Practices

California law obligates the Office of Privacy Protection, in the California Department of Consumer Affairs, to protect the privacy of individuals' personal information by "identifying consumer problems in the privacy area and facilitating [the] development of fair information practices."[12] One of the ways that the Office of Privacy Protection is directed to fulfill this mandate is by making "recommendations to organizations for privacy policies and practices that promote

and protect the interests of California consumers."[13]

The recommendations offered here are neither regulations, nor statutory mandates, nor legal opinions. Rather, they are a contribution to the development of "best practices" for businesses and other organizations to follow in managing personal information in ways that promote and protect individual privacy interests, while fostering economic development.

The Fair Information Practice Principles underlie these recommendations. Following the common path marked out by the Principles can make it easier for businesses to harmonize sometimes various privacy requirements. This approach resembles that of the U.S. Department of Commerce's "Safe Harbor" framework, which is intended to "bridge different privacy approaches and provide a streamlined means for U.S. organizations to comply with the European Union's Directive on Data Protection."[14] This approach also benefits consumers by encouraging a reduction in the number and complexity of privacy statements provided by a single business.[15]

The Office of Privacy Protection is extremely grateful for the generous work of the advisory group that assisted us on this project. The 22-member group included representatives of the banking, securities, insurance, health care, technology, telecommunications, retail, manufacturing, marketing and entertainment industries, along with consumer and privacy advocates. A list of the members of the advisory group is included as Appendix 1.

Recommended Practices

These recommendations focus on the disclosure of the details of a business's practices in sharing personal information for marketing purposes. This is but one aspect of a larger issue: the importance of providing individuals with meaningful notice of all of a business's policies and practices for managing personal information. These recommendations begin with the new California requirement that businesses disclose the details of their sharing of personal information. The recommendations address how to notify customers of their right to obtain this disclosure or the alternative customer choice opportunity. Finally the recommendations address the broader statement of a business's privacy polices and practices, including the requirements for online privacy statements.

The key terms used in this document are defined specifically for that use in the box at right.

Recommendations on the California Information-Sharing Disclosure

Provide your Information-Sharing Disclosure promptly.

- Respond to a customer's request for an Information-Sharing Disclosure as soon as possible after receiving it, but no later than within 30 days for a request made to the contact point designated in the Notice of Information-Sharing Disclosure.[16]

Make your Information-Sharing Disclosure specific and comprehensive.

- List all categories of customer personal information that you disclosed, during the past calendar year, to other companies[17] for their direct marketing purposes.
  - Consider giving examples of the types of personal information in a category. For example, contact information such

Privacy Policies and Practices: An organization's rules and procedures for collecting, using, disclosing, protecting, and managing personal information.

Privacy Policy Statement or Privacy Statement: A written statement of an organization's Privacy Policies and Practices provided or made available to individuals whose personal information is involved.

California Customer Choice Notice: A component of a company's Privacy Policy Statement that allows a customer to choose to prevent the sharing of the customer's personal information with other companies for their direct marketing purposes, as provided by California Civil Code section 1798.83.

California Information-Sharing Disclosure: A company's list of categories of customer personal information shared with other companies for direct marketing purposes and a list of companies with whom the information is shared, as required by California Civil Code section 1798.83.

California Notice of Information-Sharing Disclosure: A notice of consumers' right, under California Civil Code section 1798.83, to request and receive a copy of a company's Information-Sharing Disclosure or a cost-free means of preventing such information sharing (see Customer Choice Notice). It includes the mailing address, e-mail address, toll-free telephone number or toll-free fax number to which customers may submit a request for a company's Information-Sharing Disclosure.

Key terms are defined for use in this document.

as name, mailing address, phone number and e-mail address; financial information such as billing address, banking information, credit card information; and profile information such as interests, marital status, gender, age, or household income level.

- *Scenario*: Acme Widgets collects personal information from its customers in the following categories: Contact Information, including name, mailing address, and e-mail address; and Billing Information, including credit card account number and billing address. In 2004 Acme Widgets disclosed its customers' Contact Information to Superior Products. Superior used it to send out an offer on its new products. Acme Widgets would list in its Information-Sharing Disclosure provided in response to a request received in 2005, the following categories of personal information: Contact Information, including name, mailing address and e-mail address.

- List all other companies to which, during the past calendar year, you disclosed customer personal information for their direct marketing purposes.[18]
  - Consider listing the companies by type, such as subsidiaries and affiliates, marketing partners, market research companies, advertisers, data aggregators, etc.
  - *Scenario*: Under the facts of the previous scenario, Acme Widgets would include Superior Products in the list of companies in its Information-Sharing Disclosure, with its address and examples of Superior's products, for example, sporting goods and camping equipment.

Recommendations on the California Customer Choice Notice

If your company's published Privacy Policy Statement offers customers the right to consent to or opt out of sharing their personal information with other companies for direct marketing purposes, then provide a customer who requests an Information-Sharing Disclosure with a Customer Choice Notice allowing the customer to exercise that right at no cost.

Provide your Customer Choice Notice promptly.

- Respond to a customer's request for an Information-Sharing Disclosure by providing your Customer Choice Notice as soon as possible after receiving the request.
- Respond no later than within 30 days to a request made to the contact point designated in your Notice of Information-Sharing Disclosure.[19]

Make your Customer Choice Notice clear and understandable.[20]

- When giving a customer an opt-in choice, state clearly that you will not share personal information about the customer with other companies for their marketing use unless the customer actively consents to such sharing.
- When giving a customer an opt-out choice, use a simple check-box format and language such as "Unless you say no by checking this box, we may share personal information about you with other companies for their marketing use."[21]

Give customers a cost-free way to indicate their preference.

- Allow your customers to communicate their preferences, preferably in a manner that creates a record for you and for them: on your Web site, by e-mail, by mail, by a toll-free phone or by a toll-free fax.
- Clearly explain the extent of a customer's option not to share the customer's

information. Explain, for example, whether it applies to all relationships that a customer has with a company or to just one account.

- For example, a customer may have several bank accounts or may have signed up with a Web site several times. Explain whether the customer's preferences apply to all accounts or whether the customer needs to exercise an opt-out option for each individual account.

- It is a good idea to explain other non-marketing reasons for contacting customers, such as product safety or customer service.
  - Explain that denying consent to information sharing may not prohibit sharing for such non-marketing purposes.
- Respect your customers' preferences by keeping records and ensuring that preferences are always honored.
- Implement customer requests not to share their personal information within a reasonable time period.
  - For example, a reasonable period to implement a customer's request not to share might be within 30 to 45 days after receiving the customer's request .[22]
  - It is a good idea to inform customers of the timeframe in which they can expect that their information will no longer be shared.
  - It is a good idea to provide an acknowledgment or confirmation when a customer's request not to have personal information shared has been implemented.

Recommendations on the California Notice of Information-Sharing Disclosure

Make your Notice of Information-Sharing Disclosure recognizable.

- If the Notice is on a Web page separate from the page containing your company Privacy Statement, entitle the Notice "Your Privacy Rights" or "Your California Privacy Rights," in legible type designed to draw attention to its significance.
  - Add a link to your company's Privacy Statement at the end of the Notice.
- If the Notice is on the page containing your company Privacy Statement, put the Notice on the first linked page in a location and style that make it conspicuous.

Make your Notice of Information-Sharing Disclosure clear and understandable.[23]

- Use plain, straightforward language.
- Use titles and headers to identify key parts of the Notice.
- Use easily readable type, in a reasonably legible size and in a color that contrasts distinctly with the background.

Make your Notice of Information-Sharing Disclosure readily accessible to customers.

- Use at least one of the following means of making the Notice available to your customers. Consider using more than one.
  - Train your agents who have regular contact with your customers, and train supervisors of your customer-contact staff, in what to tell customers who request an Information-Sharing Disclosure.
    - Have your supervisors instruct employees with regular customer contact to tell customers who request an Information-Sharing Disclosure how they can get one.
  - Make your Notice of Information-Sharing Disclosure readily available at all your California locations that experience regular customer contact.

- For example, have copies of the Notice on hand at check stands or in a designated office at each location.

- Post your Notice of Information-Sharing Disclosure on your Web site.[24]
  - Post the Notice (or a conspicuous link to it) on any and all company Web sites on pages where a customer would conduct online business and on pages where a customer would reasonably expect to find information on company policies.
  - Put a conspicuous link to the Notice on the home page, that includes the words "Your Privacy Rights" or "Your California Privacy Rights."
  - On each page containing the Notice, put it in a location and style that make it conspicuous.
  - Provide a postal address, e-mail address, telephone number or fax number for the customer to contact in order to request the Information-Sharing Disclosure.

- Include a description of a customer's rights to request and receive a cost-free means of preventing such sharing of personal information or to request and receive the Information-Sharing Disclosure.

Recommendations on Privacy Statements[25]

Make your Privacy Statement recognizable.

- Whether it's printed in a brochure, posted on a Web site or enclosed with another mailing, your Privacy Statement should have a descriptive title containing the word "privacy" in legible type designed to draw attention to its significance.
- When you print your Privacy Statement, make it a separate document. On your Web site, format the Statement so that it can be printed as a separate document.
- Consider providing your Privacy Statement in languages other than English.

Make your Privacy Statement readily accessible.

- Post your Privacy Statement on your Web site(s).[26]
  - Use your Web site to make available Privacy Statements covering both your offline and online practices for managing personal information.
  - Use a conspicuous link on your home page containing the word "privacy." Make the link conspicuous by using larger type than the surrounding text, contrasting color, or symbols that call attention to it.
  - Put a conspicuous "privacy" link on every Web page where personal information is collected.
- Clearly indicate which entities a Privacy Statement covers, such as subsidiaries or affiliates.
- Make sure that employees who regularly interact with consumers and those who handle consumers' personal information understand your Privacy Statement.
- Provide copies of your Privacy Statement to new customers, regularly to all customers, and to others who request it.

Make your Privacy Statement clear and understandable.[27]

- Use plain, straightforward language. Avoid technical or legal jargon.[28]
- Use short sentences.
- Use the active voice.
- Use titles and headers to identify key

parts of the Statement. On a Web site, consider using links at the top of the page to guide users through the Statement.

- Use an easily readable type font, in a reasonably legible size and in a color that contrasts distinctly with the background.
- Invite and use customer input when drafting or revising your Privacy Statement.

Describe how you collect personal information.

- If you collect personal information from sources other than your customers, describe this in your Privacy Statement.
- If you collect personal information through Web technologies, such as cookies or Web beacons, describe this in your Privacy Statement.

Describe the kind of personal information you collect.

- Be reasonably specific in describing the kind of personal information you collect.
- At the least, list the categories of personal information that you collect from customers and from Web site visitors.[29]
    - Provide examples of the categories of personal information your company collects. For example, "We collect contact information, such as your name and e-mail address, as well as billing information, such as credit card number and billing address."

Explain how you use and share personal information.

- Explain uses of personal information beyond what is necessary for fulfilling a customer transaction.
    - Explain your practices regarding sharing of personal information with other entities, including affiliates and marketing partners.
- List the different types of companies with which you share customer personal information.[30]
    - Be sure to include any companies that have a direct link or live feed of consumer information through a Web site.

Give your customers choices on how their personal information is used or disclosed.

- Give your customers a simple, effective way to consent to, or to opt out of, sharing their personal information with other companies for marketing purposes.[31]
- Clearly explain how customers can exercise their option to withhold consent to such information sharing.
- Clearly explain the extent of a customer's option to limit sharing of personal information, for example, whether it applies to all relationships that a customer has with an organization or to just to one account.
- It is a good idea to explain other non-marketing reasons for contacting customers, such as product safety or customer service.
    - Explain that denying consent to information sharing may not prohibit sharing for non-marketing purposes, such as for completing a requested transaction.
- Respect your customers' preferences by keeping records of preferences and ensuring that they are always honored.
- Implement customer preferences within a reasonable time period.
    - For example, a reasonable period to implement a customer's denial of consent to share might be within 30 to 45 days of receiving the customer's re-

quest.[32]

- It is a good idea to let customers know the timeframe in which they can expect that their information will no longer be shared.
- It is a good idea to provide an acknowledgment or confirmation when a customer's request not to have personal information shared has been processed.

Consider offering your customers the opportunity to review and correct their personal information.

- If you do offer your customers this opportunity, explain how they can get access to their own personal information in your care.[33]
- Before providing customers access to their personal information, be sure to properly verify identity and authenticate any access right, particularly concerning sensitive personal information, such as Social Security numbers, financial account numbers, or medical information.
- Control and document customer changes or corrections to personal information., through audit logs or transaction histories, for example.

Explain how you protect your customers' personal information from unauthorized or illegal access.

- Give a general description of the security measures you use to safeguard the personal information in your care, but not in such detail as to compromise your security.
- Give a general description of the measures you use to control the information security practices of third parties with whom you share customer personal information for any purpose.

Tell your customers whom they can contact with questions or concerns about your Privacy Policies and Practices.

- Give at least a title and e-mail or postal address of a company official who will respond to privacy questions or concerns. It is a good idea to offer a telephone number, perhaps toll-free.
- Train your customer service telephone staff to recognize an inquiry about privacy. It is a good idea to make customer service staff aware of how customers can get an Information-Sharing Disclosure and a copy of your business's published Privacy Statement.
- ·Consider providing information on identity theft prevention and remediation.

Give the effective date of your Privacy Statement.[34]

- Use good version control procedures to ensure that your Privacy Statement is uniform throughout the organization.
- Explain how you will notify customers about material changes to your Privacy Policies and Practices.
  - Do not rely on merely changing the Privacy Statement on your Web site as the exclusive means of notifying customers of material changes in your uses or sharing of personal information.

Notes

[1] California Civil Code §§ 1798.83-1798.84, enacted as Chapter 505, California Statutes of 2003 (Senate Bill 27 [Figueroa]). A summary and the complete text of the law is attached as Appendix 2.

[2] California Business and Professions Code §§ 22575-22579, enacted as Chapter 829, California Statutes of 2003 (Assembly Bill 68 [Simitian]). A summary and the complete text of the law is attached as Appendix 3.

[3] The Fair Information Practice Principles, as formulated by the Organisation for Economic Co-operation and Development (OECD): Collection Limitation, Data Quality, Purpose Specification, Use Limitation, Security Safeguards, Openness, Individual Participation and Accountability.

[4] *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* and *Declaration on the Protection of Privacy in Global Networks* is available from the OECD at www.oecd.org.

[5] California Financial Information Privacy Act, Financial Code §§ 4050-4060; California Online Privacy Protection Act, Business and Professions Code §§ 22575-22579; Health Insurance Portability and Accountability Act of 1996, Standards for Privacy of Individually Identifiable Health Information, Final Rule - 45 C.F.R. Parts 160 and 164; Financial Services Modernization Act (Gramm-Leach-Bliley), Privacy Rule - 15 U.S. Code §§ 6801-6809; Safe Harbor Framework at www.export.gov/safeharbor.

[6] The survey was conducted by Privacy and American Business with Harris Interactive. The survey's results are reported in the July 2004 issue of *Privacy & American Business Newsletter*:, v. 11, no. 5, available at www.pandab.org.

[7] Ibid.

[8] 2004 Most Trusted Companies for Privacy Study, Ponemon Institute, June 10, 2004.

[9] Studies available from the Ponemon Institute at www.ponemon.org: Privacy Trust Study of the United States Government, January 11, 2004; Privacy Trust Study of the Airlines, July 11, 2004; Second Privacy Trust Study of Retail Banking, December 5, 2003; Annual Privacy Trust Study, October 31, 2003; and 2002 Privacy Trust Study of Retail Banking, October 24, 2003.

[10] Ann Cavoukian and Tyler J. Hamilton, *The Privacy Payoff*, McGraw Hill, 2002, page 303.

[11] Ponemon Institute, Attn.: Research Department, 3901 S. Escalante Ridge Place, Tucson, Arizona 85730, 520-290-3400, e-mail: research@ponemon.org.

[12] California Business and Professions Code § 350(a).

[13] California Business and Professions Code § 350(c).

[14] For more information on the Safe Harbor Framework, see the U.S. Department of Commerce's Web site at www.export.gov/safeharbor/.

[15] See the finding that more numerous and complex privacy policy documents have increased the burden on consumers, in "An Analysis of Web Site Privacy Policy Evolution in the Presence of HIPAA," by Annie I. Antón and others of the Colleges of Engineering and Management at North Carolina State University, available at www.theprivacyplace.org/.

[16] Civil Code § 1798.83(b) requires a company to respond within 30 days of receipt of a request made to the contact point provided in the Notice of Information-Sharing Disclosure. It allows up to 150 days for responding to a re-

quest made to a contact point other than the one designated in the notice.

[17] The "shine the light law" uses the term "third party," defined as one or more of the following: (A) a business that is a separate legal entity from the business that has an established business relationship with a customer, (B) a business authorized to access for its own direct marketing purposes a database shared among businesses, or (C) a business not affiliated by a common ownership or common corporate control. Civil Code § 1798.83(e)(8).

[18] The "shine the light" law, at Civil Code § 1798.83(f), allows a more limited disclosure of sharing with certain affiliated companies for direct marketing purposes. In the case of sharing with affiliates with the same brand name, a company may provide the number of affiliated companies rather than listing them all by name. And unless certain types of personal customer information are shared with such affiliates, the company does not have to list the categories of information shared. The special types of information include number, age or gender of children; personal data, such as race and religion; medical information; and financial information.

[19] See Note 16 above.

[20] See the Federal Trade Commission's advice in "Getting Noticed: Writing Effective Financial Privacy Notices," available at www.ftc.gov.

[21] See the statutory notice form in the California Financial Information Privacy Act, at Financial Code § 4053(d), as an example of a clear and understandable opt-out notice.

[22] The California Financial Information Privacy Act requires financial services companies to honor such a request within 45 days of providing an opt-out opportunity, at Financial Code § 4053(d)(3). The Federal Trade Commission's guidance on the Gramm-Leach-Bliley Act's Privacy Rule recommends 30 days as a reasonable time period.

[23] See note 20 above.

[24] See Civil Code § 1798.83(b) of the "shine the light" law for specific requirements on Web site posting of the Notice of Information-Sharing Disclosure.

[25] Among those businesses required by law to make a statement of their privacy policies and practices available to customers and others are operators of commercial Web sites or online services that collect personal information on California residents (California Online Privacy Protection Act); specified financial services companies (California Financial Information Privacy Act and the federal Gramm-Leach-Bliley Act); health care providers, health plans and health clearinghouses (Health Insurance Portability and Access Act); and certain companies doing business in Europe (Safe Harbor, EU Data Protection Directive).

[26] Operators of commercial Web sites and online services that collect personal information on California residents are required by the California Online Privacy Protection Act to "conspicuously post" a privacy statement on the Web site. Business and Professions Code § 22577(b) defines "conspicuously post" with specific examples that would make the statement noticeable by a reasonable person.

[27] See Note 20 above.

[28] According to the National Adult Literacy Survey, about half of American adults function at a level that makes reading more than brief, uncomplicated texts very difficult. Readability measures are based on average sentence length and average number of words per sentence. One standard for a readable privacy notice is set in the California Financial Information Privacy Act (Financial Code § 4053(d)), which requires a minimum Flesch reading ease score of 50, or Fairly Difficult. Compare this to the simpler Plain English level, which has a Flesch score of 65, based on an average sentence length of 15 to 20 words or less and an average word length of two syllables.

[29] Operators of commercial Web sites and of online services that collect personal information on California residents are required by the Online Privacy Protection Act to include in their privacy statement a list of categories of personal

information collected online. California Business and Professions Code § 22575(b)(1).

[30] The Online Privacy Protection Act requires operators of commercial Web sites and of online services that collect personal information on California residents to include in their privacy statement a list of the categories of "third parties" with whom personal information on California residents is shared. California Business and Professions Code § 22575(b)(1).

[31] The "shine the light" law, at California Civil Code § 1798.83(c), allows a company subject to its provisions to respond to a customer request for an Information-Sharing Disclosure by providing the customer with a cost-free opportunity to prevent such information sharing with third parties for marketing purposes. The company must adopt and disclose this policy to the public, which would include publishing it in its privacy statement.

[32] See Note 22 above.

[33] The Online Privacy Protection Act., at California Business and Professions Code § 22575(b)(2), requires operators of commercial Web sites and of online services to provide a description of the process for reviewing and correcting personal information, where such a process is offered.

[34] The Online Privacy Protection Act., at California Business and Professions Code § 22575(b)(3), requires operators of commercial Web sites and of online services to provide a policy effective date and a description of the means of notifying customers and others of material changes to the policy.

Appendix 1: Advisory Group

Jonathan Avila
The Walt Disney Company

Joanne Bettancourt
Securities Industry Association

Steve Blackledge
CALPIRG

Kaye Caldwell
Internet Alliance

Keith Cheresko
Ford

Ann Eowan
Association of California Life and Health Insurance Companies

Jonathan Fox
Sun Microsystems

Mari Frank
Attorney, Privacy Consultant, Author

Joanne Furtsch
TRUSTe

Leanne Gassaway
California Association of Health Plans

Beth Givens
Privacy Rights Clearinghouse

Roxanne Gould
American Electronics Association

Mike Griffiths
Albertsons
California Retailers Association

Charles Halnan
The Direct Marketing Association

Ed Howard
Office of Senator Liz Figueroa

Peter McCorkell
Wells Fargo Bank
California Bankers Association

Valerie Nera
California Chamber of Commerce

Deborah Pierce
PrivacyActivism

Larry Ponemon
Ponemon Institute

Kathy Rehmer
Cingular

Saundra Kae Rubel
Jefferson Data Strategies, LLC

Sam Sorich
National Association of Independent Insurers

Appendix 2: California's "Shine the Light" Law

Summary of the Law's Requirements

Which Businesses Are Subject to the Statute

California Civil Code section 1798.83 imposes a specific disclosure requirement on many businesses[1] that share their customers' personal information with other businesses for direct marketing purposes. It applies to businesses that have the following:

- 20 or more employees,
- An established business relationship with a customer who is a California resident, and
- Within the immediately preceding calendar year, shared customer personal information with other companies for their direct marketing use.

The statute exempts from its requirements: (1) financial institutions that are subject to certain provisions of the California Financial Information Privacy Act,[2] and (2) specific types of business-related disclosures to third parties, such as those for administration or customer service, provided that the third parties do not use the information for their own direct marketing purposes.

Notifying Customers of Their Rights Under the Statute

Businesses must notify California customers of their rights under the statute by designating a contact point (mailing address, e-mail address, toll-free phone number or toll-free fax number) for customers to contact to request a business's disclosure regarding how it shares personal information with other businesses for direct marketing purposes ("California Information-Sharing Disclosure").

In at least one of three ways, a business must notify customers of the contact point for requesting the business's Information-Sharing Disclosure:

1. Tell agents and supervisors of customer-contact staff to instruct employees about giving contact point information to customers who request a business's Information-Sharing Disclosure.
2. On the business's Web site, provide information on the contact point and describe customer rights.
   - Link on home page using words "Your Privacy Rights" or "Your California Privacy Rights" to another Web page or to the page that contains the business's Privacy Policy Statement.
   - First linked page from the "Your Privacy Rights" link must describe a customer's rights to request and receive an Information-Sharing Disclosure or a cost-free means of preventing such disclosures, and must provide information on the business's contact point for making such a request.
3. Make information on the contact point readily accessible at all California locations with regular customer contact.

What Information a Business Must Disclose

In response to a request from a California customer for an Information-Sharing Disclosure, a company must do one of the following, once in a calendar year for each requesting customer:

- Provide in writing or by e-mail, at no cost to the customer, the following Information-Sharing Disclosure:
  - A list of categories of personal information shared, during the immediately preceding calendar year, with other businesses for their direct marketing purposes, and
  - Names and addresses of other businesses with whom such information was shared, if needed to indicate nature of business, with examples of products or services

  OR
- If the business has a published privacy policy of not sharing personal information with other companies for direct marketing purposes without customer consent (opt-in or opt-out), then provide a notice of the customer's right to prevent such sharing together with a cost-free means of doing so ("California Customer Choice Notice").

Responding to a Customer Request

A business must respond to a request from a California customer for an Information-Sharing Disclosure:

- In response to a customer's request made to the designated contact point, provide Information-Sharing Disclosure or Customer Choice Notice, within 30 days of receipt of request.
- In response to a customer's request made to another address, provide Information-Sharing Disclosure or Customer Choice Notice, in "reasonable time period," no later than 150 days from receipt of request.

If information about the business's contact point is provided on the business's Web site via a home page link that includes the words "Your California Privacy Rights," the business need not respond to requests made to any address other than the address so provided.

Remedies and Penalties

- Private right of action for damages, injunctive relief, civil penalties of up to $500 per violation.
- Willful, intentional or reckless violation: damages, injunctive relief, civil penalty of up to $3,000 per violation
- A prevailing plaintiff is entitled to recover reasonable attorney fees and costs.
- Unless violation is willful, intentional or reckless, a business may assert as a complete defense that it provided accurate, complete information within 90 days of knowing of inadequacy.

Text of California Civil Code Sections 1798.83-1798.84

1798.83. (a) Except as otherwise provided in subdivision (d), if a business has an established business relationship with a customer and has within the immediately preceding calendar year disclosed personal information that corresponds to any of the categories of personal information set forth in paragraph (6) of subdivision (e) to third parties, and if the business knows or reasonably should know that the third parties used the personal information for the third parties' direct marketing purposes, that business shall, after the receipt of a written or electronic mail request, or, if the business chooses to receive requests by toll-free telephone or facsimile numbers, a telephone or facsimile request from the customer, provide all of the following information to the customer free of charge:

(1) In writing or by electronic mail, a list of the categories set forth in paragraph (6) of subdivision (e) that correspond to the personal information disclosed by the business to third parties for the third parties' direct marketing purposes during the immediately preceding calendar year.

(2) In writing or by electronic mail, the names and addresses of all of the third parties that received personal information from the business for the third parties' direct marketing purposes during the preceding calendar year and, if the nature of the third parties' business cannot reasonably be determined from the third parties' name, examples of the products or services marketed, if known to the business, sufficient to give the customer a reasonable indication of the nature of the third parties' business.

(b) (1) A business required to comply with this section shall designate a mailing address, electronic mail address, or, if the business chooses to receive requests by telephone or facsimile, a toll-free telephone or facsimile number, to which customers may deliver requests pursuant to subdivision (a). A business required to comply with this section shall, at its election, do at least one of the following:

(A) Notify all agents and managers who directly supervise employees who regularly have contact with customers of the designated addresses or numbers or the means to obtain those addresses or numbers and instruct those employees that customers who inquire about the business' privacy practices or the business' compliance with this section shall be informed of the designated addresses or numbers or the means to obtain the addresses or numbers.

(B) Add to the home page of its Web site, a link either to a page titled "Your Privacy Rights" or to add the words "Your Privacy Rights," to the home page's link to the business' privacy policy. If the business elects to add the words "Your Privacy Rights" to the link to the business' privacy policy, the words "Your Privacy Rights" shall be in the same style and size of the link to the business' privacy policy. If the business does not display a link to its privacy policy on the home page of its Web site, or does not have a privacy policy, the words "Your Privacy Rights" shall be written in larger type than the surrounding text, or in contrasting type, font, or color to the surrounding text of the same size, or set off from the surrounding text of the same size by symbols or other marks that call attention to the language. The first page of the link shall describe a customer's rights pursuant to this section and shall provide the designated mailing address, e-mail address, as required, or toll-free telephone number or facsimile number, as appropriate. If the business elects to add the words "Your California Privacy Rights" to the home page's link to the business's privacy policy in a manner that complies with this subdivision, and the first page of the link describes a customer's rights pursuant to this section, and provides the designated mailing address, electronic mailing address, as required, or toll-free telephone or facsimile number, as appropriate, the business need not respond to requests that are not received at one of the designated addresses or numbers.

(C) Make the designated addresses or numbers, or means to obtain the designated addresses or numbers, readily available upon request of a customer at every place of business in California where the business or its agents regularly have contact with customers.

The response to a request pursuant to this section received at one of the designated addresses or numbers shall be provided within 30 days. Requests received by the business at other than one of the designated addresses or numbers shall be provided within a reasonable period, in light of the circumstances related to how the request was received, but not to exceed 150 days from the date received.

(2) A business that is required to comply with this section and Section 6803 of Title 15 of the United States Code may comply with this section by providing the customer the disclosure required by Section 6803 of Title 15 of the United States Code, but only if the disclosure also complies with this section.

(3) A business that is required to comply with this section is not obligated to provide information associated with specific individuals and may provide the information required by this section in standardized format.

(c) (1) A business that is required to comply with this section is not obligated to do so in re-

sponse to a request from a customer more than once during the course of any calendar year. A business with fewer than 20 full-time or part-time employees is exempt from the requirements of this section.

(2) If a business that is required to comply with this section adopts and discloses to the public, in its privacy policy, a policy of not disclosing personal information of customers to third parties for the third parties' direct marketing purposes unless the customer first affirmatively agrees to that disclosure, or of not disclosing the personal information of customers to third parties for the third parties' direct marketing purposes if the customer has exercised an option that prevents that information from being disclosed to third parties for those purposes, as long as the business maintains and discloses the policies, the business may comply with subdivision (a) by notifying the customer of his or her right to prevent disclosure of personal information, and providing the customer with a cost free means to exercise that right.

(d) The following are among the disclosures not deemed to be disclosures of personal information by a business for a third parties' direct marketing purposes for purposes of this section:

(1) Disclosures between a business and a third party pursuant to contracts or arrangements pertaining to any of the following:

(A) The processing, storage, management, or organization of personal information, or the performance of services on behalf of the business during which personal information is disclosed, if the third party that processes, stores, manages, or organizes the personal information does not use the information for a third party's direct marketing purposes and does not disclose the information to additional third parties for their direct marketing purposes.

(B) Marketing products or services to customers with whom the business has an established business relationship where, as a part of the marketing, the business does not disclose personal information to third parties for the third parties' direct marketing purposes.

(C) Maintaining or servicing accounts, including credit accounts and disclosures pertaining to the denial of applications for credit or the status of applications for credit and processing bills or insurance claims for payment.

(D) Public record information relating to the right, title, or interest in real property or information relating to property characteristics, as defined in Section 408.3 of the Revenue and Taxation Code, obtained from a governmental agency or entity or from a multiple listing service, as defined in Section 1087, and not provided directly by the customer to a business in the course of an established business relationship.

(E) Jointly offering a product or service pursuant to a written agreement with the third party that receives the personal information, provided that all of the following requirements are met:

(i) The product or service offered is a product or service of, and is provided by, at least one of the businesses that is a party to the written agreement.

(ii) The product or service is jointly offered, endorsed, or sponsored by, and clearly and conspicuously identifies for the customer, the businesses that disclose and receive the disclosed personal information.

(iii) The written agreement provides that the third party that receives the personal information is required to maintain the confidentiality of the information and is prohibited from disclosing or using the information other than to carry out the joint offering or servicing of a product or service that is the subject of the written agreement.

(2) Disclosures to or from a consumer reporting agency of a customer's payment history or other information pertaining to transactions or experiences between the business and a customer if that information is to be reported in, or used to generate, a consumer report as defined in subdivision (d) of Section 1681a of Title 15 of the United States Code, and use of that information is limited by the federal Fair Credit Reporting Act.

(3) Disclosures of personal information by a

business to a third party financial institution solely for the purpose of the business obtaining payment for a transaction in which the customer paid the business for goods or services with a check, credit card, charge card, or debit card, if the customer seeks the information required by subdivision (a) from the business obtaining payment, whether or not the business obtaining payment knows or reasonably should know that the third party financial institution has used the personal information for its direct marketing purposes.

(4) Disclosures of personal information between a licensed agent and its principal, if the personal information disclosed is necessary to complete, effectuate, administer, or enforce transactions between the principal and the agent, whether or not the licensed agent or principal also uses the personal information for direct marketing purposes, if that personal information is used by each of them solely to market products and services directly to customers with whom both have established business relationships as a result of the principal and agent relationship.

(5) Disclosures of personal information between a financial institution and a business that has a private label credit card, affinity card, retail installment contract, or co-branded card program with the financial institution, if the personal information disclosed is necessary for the financial institution to maintain or service accounts on behalf of the business with which it has a private label credit card, affinity card, retail installment contract, or branded card program, or to complete, effectuate, administer, or enforce customer transactions or transactions between the institution and the business, whether or not the institution or the business also uses the personal information for direct marketing purposes, if that personal information is used solely to market products and services directly to customers with whom both the business and the financial institution have established business relationships as a result of the private label credit card, affinity card, retail installment contract, or co-branded card program.

(e) For purposes of this section:

(1) "Customer" means an individual who is a resident of California who provides personal information to a business during the creation of, or throughout the duration of, an established business relationship if the business relationship is primarily for personal, family, or household purposes.

(2) "Direct marketing purposes" means the use of personal information to solicit or induce a purchase, rental, lease, or exchange of products, goods, property, or services directly to individuals by means of the mail, telephone, or electronic mail for their personal, family, or household purposes. The sale, rental, exchange, or lease of personal information for consideration to businesses is a direct marketing purpose of the business that sells, rents, exchanges or obtains consideration for the personal information. "Direct marketing purposes" does not include the use of personal information (A) by bona fide tax exempt charitable or religious organizations to solicit charitable contributions, (B) to raise funds from and communicate with individuals regarding politics and government, (C) by a third party when the third party receives personal information solely as a consequence of having obtained for consideration permanent ownership of accounts that might contain personal information, or (D) by a third party when the third party receives personal information solely as a consequence of a single transaction where, as a part of the transaction, personal information had to be disclosed in order to effectuate the transaction.

(3) "Disclose" means to disclose, release, transfer, disseminate, or otherwise communicate orally, in writing, or by electronic or any other means to any third party.

(4) "Employees who regularly have contact with customers" means employees whose contact with customers is not incidental to their primary employment duties, and whose duties do not predominantly involve ensuring the safety or health of the businesses customers. It includes, but is not limited to, employees whose primary employment duties are as cashier, clerk, customer ser-

vice, sales, or promotion. It does not, by way of example, include employees whose primary employment duties consist of food or beverage preparation or service, maintenance and repair of the business' facilities or equipment, direct involvement in the operation of a motor vehicle, aircraft, watercraft, amusement ride, heavy machinery or similar equipment, security, or participation in a theatrical, literary, musical, artistic, or athletic performance or contest.

(5) "Established business relationship" means a relationship formed by a voluntary, two-way communication between a business and a customer, with or without an exchange of consideration, for the purpose of purchasing, renting, or leasing real or personal property, or any interest therein, or obtaining a product or service from the business, if the relationship is ongoing and has not been expressly terminated by the business or the customer, or if the relationship is not ongoing, but is solely established by the purchase, rental, or lease of real or personal property from a business, or the purchase of a product or service, no more than 18 months have elapsed from the date of the purchase, rental, or lease.

(6) (A) The categories of personal information required to be disclosed pursuant to paragraph (1) of subdivision (a) are all of the following:

(i) Name and address.

(ii) Electronic mail address.

(iii) Age or date of birth.

(iv) Names of children.

(v) Electronic mail or other addresses of children.

(vi) Number of children.

(vii) The age or gender of children.

(viii) Height.

(ix) Weight.

(x) Race.

(xi) Religion.

(xii) Occupation.

(xiii) Telephone number.

(xiv) Education.

(xv) Political party affiliation.

(xvi) Medical condition.

(xvii) Drugs, therapies, or medical products or equipment used.

(xviii) The kind of product the customer purchased, leased, or rented.

(xix) Real property purchased, leased, or rented.

(xx) The kind of service provided.

(xxi) Social security number.

(xxii) Bank account number.

(xxiii) Credit card number.

(xxiv) Debit card number.

(xxv) Bank or investment account, debit card, or credit card balance.

(xxvi) Payment history.

(xxvii) Information pertaining to the customer's creditworthiness, assets, income, or liabilities.

(B) If a list, description, or grouping of customer names or addresses is derived using any of these categories, and is disclosed to a third party for direct marketing purposes in a manner that permits the third party to identify, determine, or extrapolate any other personal information from which the list was derived, and that personal information when it was disclosed identified, described, or was associated with an individual, the categories set forth in this subdivision that correspond to the personal information used to derive the list, description, or grouping shall be considered personal information for purposes of this section.

(7) "Personal information" as used in this section means any information that when it was disclosed identified, described, or was able to be associated with an individual and includes all of the following:

(A) An individual's name and address.

(B) Electronic mail address.

(C) Age or date of birth.

(D) Names of children.

(E) Electronic mail or other addresses of children.

(F) Number of children.

(G) The age or gender of children.

(H) Height.

(I) Weight.

(J) Race.

(K) Religion.

(L) Occupation.
(M) Telephone number.
(N) Education.
(O) Political party affiliation.
(P) Medical condition.
(Q) Drugs, therapies, or medical products or equipment used.
(R) The kind of product the customer purchased, leased, or rented.
(S) Real property purchased, leased, or rented.
(T) The kind of service provided.
(U) Social security number.
(V) Bank account number.
(W) Credit card number.
(X) Debit card number.
(Y) Bank or investment account, debit card, or credit card balance.
(Z) Payment history.
(AA) Information pertaining to creditworthiness, assets, income, or liabilities.

(8) "Third party" or "third parties" means one or more of the following:

(A) A business that is a separate legal entity from the business that has an established business relationship with a customer.

(B) A business that has access to a database that is shared among businesses, if the business is authorized to use the database for direct marketing purposes, unless the use of the database is exempt from being considered a disclosure for direct marketing purposes pursuant to subdivision (d).

(C) A business not affiliated by a common ownership or common corporate control with the business required to comply with subdivision (a).

(f) (1) Disclosures of personal information for direct marketing purposes between affiliated third parties that share the same brand name are exempt from the requirements of paragraph (1) of subdivision (a) unless the personal information disclosed corresponds to one of the following categories, in which case the customer shall be informed of those categories listed in this subdivision that correspond to the categories of personal information disclosed for direct marketing purposes and the third party recipients of personal information disclosed for direct marketing purposes pursuant to paragraph (2) of subdivision (a):

(A) Number of children.
(B) The age or gender of children.
(C) Electronic mail or other addresses of children.
(D) Height.
(E) Weight.
(F) Race.
(G) Religion.
(H) Telephone number.
(I) Medical condition.
(J) Drugs, therapies, or medical products or equipment used.
(K) Social security number.
(L) Bank account number.
(M) Credit card number.
(N) Debit card number.
(O) Bank or investment account, debit card, or credit card balance.

(2) If a list, description, or grouping of customer names or addresses is derived using any of these categories, and is disclosed to a third party or third parties sharing the same brand name for direct marketing purposes in a manner that permits the third party to identify, determine, or extrapolate the personal information from which the list was derived, and that personal information when it was disclosed identified, described, or was associated with an individual, any other personal information that corresponds to the categories set forth in this subdivision used to derive the list, description, or grouping shall be considered personal information for purposes of this section.

(3) If a business discloses personal information for direct marketing purposes to affiliated third parties that share the same brand name, the business that discloses personal information for direct marketing purposes between affiliated third parties that share the same brand name may comply with the requirements of paragraph (2) of subdivision (a) by providing the overall number of affiliated companies that share the same brand name.

(g) The provisions of this section are severable. If any provision of this section or its application is held invalid, that invalidity shall not affect other provisions or applications that can be given effect without the invalid provision or application.

(h) This section does not apply to a financial institution that is subject to the California Financial Information Privacy Act (Division 1.2 (commencing with Section 4050) of the Financial Code) if the financial institution is in compliance with Sections 4052, 4025, 4053, 4053.5 and 4054.6 of the Financial Code, as those sections read when they were chaptered on August 28, 2003, and as subsequently amended by the Legislature or by initiative.

(i) This section shall become operative on January 1, 2005.

1798.84. (a) Any waiver of a provision of this title is contrary to public policy and is void and unenforceable.

(b) Any customer injured by a violation of this title may institute a civil action to recover damages.

(c) In addition, for a willful, intentional, or reckless violation of Section 1798.83, a customer may recover a civil penalty not to exceed three thousand dollars ($3,000) per violation; otherwise, the customer may recover a civil penalty of up to five hundred dollars ($500) per violation for a violation of Section 1798.83.

(d) Unless the violation is willful, intentional, or reckless, a business that is alleged to have not provided all the information required by subdivision (a) of Section 1798.83, to have provided inaccurate information, failed to provide any of the information required by subdivision (a) of Section 1798.83, or failed to provide information in the time period required by subdivision (b) of Section 1798.83, may assert as a complete defense in any action in law or equity that it thereafter provided regarding the information that was alleged to be untimely, all the information, or accurate information, to all customers who were provided incomplete or inaccurate information, respectively, within 90 days of the date the business knew that it had failed to provide the information, timely information, all the information, or the accurate information, respectively.

(e) Any business that violates, proposes to violate, or has violated this title may be enjoined.

(f) A prevailing plaintiff in any action commenced under Section 1798.83 shall also be entitled to recover his or her reasonable attorney's fees and costs.

(g) The rights and remedies available under this section are cumulative to each other and to any other rights and remedies available under law.

Notes

[1] Civil Code, § 1798.80, defines "business" as "a sole proprietorship, partnership, corporation, association, or other group, however organized and whether or not organized to operate at a profit, including a financial institution organized, chartered, or holding a license or authorization certificate under the law of this state, any other state, the United States, or of any other country, or the parent or the subsidiary of a financial institution. The term includes an entity that destroys records."

[2] See Civil Code, § 1798.83(h), which exempts financial institutions that are subject to and in compliance with Financial Code, §§ 4052, 4053, 4053.5 and 4054.6.

Appendix 3: California Online Privacy Protection Act

Summary of the Laws's Requirements

Which Businesses Are Subject to the Statute

Operators of commercial Web sites or online services that collect personally identifiable information on consumers residing in California.

"Personally identifiable information" is defined as:

- individually identifiable information about a consumer collected online from the individual and maintained by the operator,
  - including name, address, e-mail address, telephone number, Social Security number, any other identifier that permits the physical or online contacting of an individual, and information concerning a user collected from the user in combination with another identifier.

What Operators Must Do Under the Statute

An operator of a commercial Web sites or online service must do the following:

- conspicuously post a privacy policy statement containing specified information on its Web site, and
- comply with the terms of that policy.

The posted policy must contain the following information:

- Categories of personally identifiable information collected
- Categories of third parties with whom the information may be shared
- Description of the process, if one is offered, for reviewing one's own information collected through the site
- Description of the process for communicating material changes in the policy
- Effective date of the policy

"Conspicuously post" means any of the following:

- Posting on a Web site's home page or first significant page after entering the site
- Posting a link to the policy containing the word "privacy" on the Web site's home page or first significant page
- Making the link conspicuous by including the word "privacy," using capital letters in larger type than surrounding text, using type that contrasts with surrounding text in size, style or color or that is set off by marks that call attention to it, or by using any other functional hyperlink that a reasonable person would notice.
- An online service may use any reasonable means of making the privacy policy available to consumers of the service.

Remedies and Penalties

- An operator has a 30-day grace period after being notified of failure to post a policy that complies with the law.
- An operator subject to the law is in violation for failing to comply either "knowingly and willfully" or "negligently and materially."

- The law may be enforced through California's unfair competition statute, Business and Professions Code section 17200 and following.

Text of Business and Professions Code Sections 22575-22579

22575. (a) An operator of a commercial Web site or online service that collects personally identifiable information through the Internet about individual consumers residing in California who use or visit its commercial Web site or online service shall conspicuously post its privacy policy on its Web site, or in the case of an operator of an online service, make that policy available in accordance with paragraph (5) of subdivision (b) of Section 22578.

An operator shall be in violation of this subdivision only if the operator fails to post its policy within 30 days after being notified of noncompliance.

(b) The privacy policy required by subdivision (a) shall do all of the following:

(1) Identify the categories of personally identifiable information that the operator collects through the Web site or online service about individual consumers who use or visit its commercial Web site or online service and the categories of third-party persons or entities with whom the operator may share that personally identifiable information.

(2) If the operator maintains a process for an individual consumer who uses or visits its commercial Web site or online service to review and request changes to any of his or her personally identifiable information that is collected through the Web site or online service, provide a description of that process.

(3) Describe the process by which the operator notifies consumers who use or visit its commercial Web site or online service of material changes to the operator's privacy policy for that Web site or online service.

(4) Identify its effective date.

22576. An operator of a commercial Web site or online service that collects personally identifiable information through the Web site or online service from individual consumers who use or visit the commercial Web site or online service and who reside in California shall be in violation of this section if the operator fails to comply with the provisions of Section 22575 or with the provisions of its posted privacy policy in either of the following ways:

(a) Knowingly and willfully.

(b) Negligently and materially.

22577. For the purposes of this chapter, the following definitions apply:

(a) The term "personally identifiable information" means individually identifiable information about an individual consumer collected online by the operator from that individual and maintained by the operator in an accessible form, including any of the following:

(1) A first and last name.

(2) A home or other physical address, including street name and name of a city or town.

(3) An e-mail address.

(4) A telephone number.

(5) A social security number.

(6) Any other identifier that permits the physical or online contacting of a specific individual.

(7) Information concerning a user that the Web site or online service collects online from the user and maintains in personally identifiable form in combination with an identifier described in this subdivision.

(b) The term "conspicuously post" with respect to a privacy policy shall include posting the privacy policy through any of the following:

(1) A Web page on which the actual privacy policy is posted if the Web page is the homepage or first significant page after entering the Web site.

(2) An icon that hyperlinks to a Web page on which the actual privacy policy is posted, if the icon is located on the homepage or the first significant page after entering the Web site, and if the icon contains the word "privacy." The icon shall also use a color that contrasts with the background color of the Web page or is otherwise

distinguishable.

(3) A text link that hyperlinks to a Web page on which the actual privacy policy is posted, if the text link is located on the homepage or first significant page after entering the Web site, and if the text link does one of the following:

(A) Includes the word "privacy."

(B) Is written in capital letters equal to or greater in size than the surrounding text.

(C) Is written in larger type than the surrounding text, or in contrasting type, font, or color to the surrounding text of the same size, or set off from the surrounding text of the same size by symbols or other marks that call attention to the language.

(4) Any other functional hyperlink that is so displayed that a reasonable person would notice it.

(5) In the case of an online service, any other reasonably accessible means of making the privacy policy available for consumers of the online service.

(c) The term "operator" means any person or entity that owns a Web site located on the Internet or an online service that collects and maintains personally identifiable information from a consumer residing in California who uses or visits the Web site or online service if the Web site or online service is operated for commercial purposes. It does not include any third party that operates, hosts, or manages, but does not own, a Web site or online service on the owner's behalf or by processing information on behalf of the owner.

(d) The term "consumer" means any individual who seeks or acquires, by purchase or lease, any goods, services, money, or credit for personal, family, or household purposes.

22578. It is the intent of the Legislature that this chapter is a matter of statewide concern. This chapter supersedes and preempts all rules, regulations, codes, ordinances, and other laws adopted by a city, county, city and county, municipality, or local agency regarding the posting of a privacy policy on an Internet Web site.

22579. This chapter shall become operative on July 1, 2004.