MAKING YOUR PRIVACY PRACTICES PUBLIC

Kamala D. Harris, Attorney General
California Department of Justice

MAKING YOUR
PRIVACY PRACTICES
PUBLIC

Recommendations on Developing a Meaningful Privacy Policy

May 2014

Kamala D. Harris, Attorney General
California Department of Justice

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Meaningful privacy policy statements safeguard consumers by helping them make informed decisions about which companies they will entrust with their personal information. They are also an opportunity for companies to build their brands and to develop goodwill and trust through transparency. Many privacy policies, however, are overly long and difficult to read without offering meaningful choices to consumers. Indeed, research shows that consumers do not understand, and many do not even read, the privacy policies on the web sites they visit.

The Attorney General's Office, in furtherance of its mission to protect the inalienable right to privacy conferred by the California Constitution, offers these recommendations to support companies in their work to provide privacy policy statements that are meaningful to consumers. To be specific, the guidance set forth here is intended to encourage companies to craft privacy policy statements that address significant data collection and use practices, use plain language, and are presented in a readable format.

The California Online Privacy Protection Act of 2003 (CalOPPA), the first law in the nation with a broad requirement for privacy policies, is a privacy landmark. The Act applies to operators of commercial web sites and online services that collect personally identifiable information about Californians. It requires them to say what they do and do what they say—to conspicuously post a privacy policy and to comply with it. The Act was amended in 2013 to address the issue of online tracking—the collection of personal information about consumers as they move across web sites and online services. Do Not Track (DNT) technology exists, enabling consumers to communicate their desire not to be tracked through their browsers. However, many consumers do not know how sites and services are responding to their browsers' Do Not Track signals. The 2013 amendments to CalOPPA require web site operators and online services to inform consumers of just this, and the recommendations set forth here address these new provisions.

This document is another of the Attorney General's recommendations on privacy and security practices, including the recently released *Cybersecurity in the Golden State*.

HIGHLIGHTS OF RECOMMENDATIONS

Readability

- Use plain, straightforward language. Avoid technical or legal jargon.
- Use a format that makes the policy readable, such as a layered format.

Online Tracking/Do Not Track

- Make it easy for a consumer to find the section in which you describe your policy regarding online tracking by labeling it, for example: “How We Respond to Do Not Track Signals,” “Online Tracking” or “California Do Not Track Disclosures.”
- Describe how you respond to a browser’s Do Not Track signal or to other such mechanisms. This is more transparent than linking to a “choice program.”
- State whether other parties are or may be collecting personally identifiable information of consumers while they are on your site or service.

Data Use and Sharing

- Explain your uses of personally identifiable information beyond what is necessary for fulfilling a customer transaction or for the basic functionality of an online service.
- Whenever possible, provide a link to the privacy policies of third parties with whom you share personally identifiable information.

Individual Choice and Access

- Describe the choices a consumer has regarding the collection, use and sharing of his or her personal information.

Accountability

- Tell your customers whom they can contact with questions or concerns about your privacy policies and practices.

INTRODUCTION

Recommended Practices: Purpose and Scope

The Attorney General's Privacy Enforcement and Protection Unit has the mission of protecting the inalienable right to privacy conferred by the California Constitution. The Privacy Unit enforces state and federal privacy laws and develops programs to educate individuals, businesses and organizations on privacy rights and best practices.

The Attorney General's Office regularly receives requests for information on drafting privacy policy statements, often from smaller companies and organizations. These recommendations are intended to respond to such requests and to encourage companies and other organizations to provide meaningful privacy policy statements. A meaningful privacy policy statement addresses significant data collection and use practices, uses plain language, and is presented in a format that enhances its readability. The recommendations here, which in some places offer greater privacy protection than required by existing law, are not regulations, mandates or legal opinions. Rather, they are part of an effort to encourage the development of privacy best practices.

In developing this document, the Privacy Unit consolidated previously published recommendations on aspects of privacy policy statements (namely, *Privacy on the Go: Recommendations for the Mobile Ecosystem* and the California Office of Privacy Protection's *Recommended Practices on California Information-Sharing Disclosures and Privacy Policy Statements*), both of which are available in the Business Resources section of the Attorney General's Privacy web site at www.oag.ca.gov/privacy. We have now added a new section on disclosures related to online tracking and response to Do Not Track mechanisms.

In formulating our tracking transparency recommendations, we consulted numerous stakeholders from various business sectors, as well as academics and privacy advocates. We appreciate their contributions.

Transparency and Privacy

Transparency is one of the Fair Information Practice Principles that underlie privacy laws and regulations around the world. The Organisation for Economic Cooperation and Development calls for transparency "about developments, practices and policies with respect to personal data," as one of the guidelines intended to help harmonize national privacy legislation while supporting the data flow essential to international commerce.[1]

Lawmakers in the United States began addressing the issue in the 1970s with the passage of the Fair Credit Reporting Act, America's first information privacy statute, which opened up the formerly opaque practices of the consumer credit industry to the consumers whose personal information is its raw material.[2] Soon afterwards, the federal Privacy Act of 1974 created a system of privacy policy documentation that made the data practices of federal agencies available to the public.[3] In the 1990s, major federal laws were enacted requiring privacy policy statements from the healthcare and financial services industries and from web sites and online services directed to children under the age of 13.[4] California's Online Privacy Protection Act of 2003 was the first law in the nation to require operators of commercial web sites and online services to post a privacy policy.[5] While the law only applies to companies that collect personally identifiable information of California residents, the state's economic importance and the borderless world of online commerce extend the impact of this law to other jurisdictions.

As the result of these laws and marketplace forces, most web sites now post some sort of privacy policy statement, most commonly accessed by a link labeled with the word "privacy" found at the bottom of the home page or even every page. And, as a result of recent efforts by the California Attorney General, such as *Privacy on the Go: Recommendations for the Mobile Ecosystem* (2013), available at www.oag.ca.gov/privacy, more mobile apps make privacy policies available.

Transparency is also related to trust. Studies of privacy trust identify disclosures of privacy and security practices as one of the key factors that build trust in a company.[6] And it is often a lack of transparency that exacerbates public concern—and generates headlines—when unexpected data practices are revealed.

Privacy Policy Statements and Privacy Notices

While there is little debate about the centrality of transparency in empowering individuals to make informed decisions, there is less agreement on the best way to make data practices transparent. Dissatisfaction with the effectiveness of privacy policy statements has grown over time. As the use of personal information in commerce has expanded in scope and complexity, comprehensive privacy policy statements have tended to become lengthier and more legalistic in style, yet often fail to address data handling practices of concern to consumers or offer them meaningful choices about the collection and use of their data.[7] The typical policy's ineffectiveness as a consumer communication tool has been borne out by research findings that consumers do not understand, and many do not even read, the privacy policies on the web sites they visit.[8]

The Federal Trade Commission (FTC) has called for improved data practice transparency, encouraging privacy policy statements that are "clearer, shorter, and more standardized to enable better comprehension and comparison of privacy practices."[9] The White House has also made greater transparency one of the cornerstones of a proposed Consumer Privacy Bill of Rights, calling for "plain language statements about personal data collection [and] use."[10]

These government authorities and academic researchers have proposed various ways to make general privacy policy statements more meaningful and effective. They have recommended alternative formats, such as a layered format that highlights the most relevant privacy issues and a standardized grid or "nutrition label" format that facilitates comparison of different companies' policies. They have also encouraged stakeholders to collaborate on standardized terminology and icons to improve comprehension.[11]

Another recommended approach is to supplement a comprehensive privacy policy with simpler, shorter privacy notices to alert consumers to potentially unexpected data practices. Rather than describing the full range of data practices, such a privacy notice would be delivered in context and "just-in-time," and would address a specific practice. For example, mobile device operating systems that use location data often deliver a notice just before collecting the location data and give users an opportunity to allow or prevent the practice.[12]

In *Privacy on the Go: Recommendations for the Mobile Ecosystem*, the California Attorney General recommended a "surprise minimization" approach whereby a mobile app would supplement its comprehensive privacy policy statement with shorter special notices regarding the collection of personally

identifiable information not necessary for the app's basic functionality or sensitive information, such as medical or financial information. The multi-stakeholder process facilitated by the National Telecommunications and Information Administration resulted in a supplemental short form notice for mobile apps, another example of a privacy notice that focuses on practices likely to be of concern to consumers.[13]

Shorter, contextual privacy notices hold great promise, particularly in the limited space available in mobile devices and other embedded technologies. But there is still an important role for the comprehensive privacy policy statement that provides a fuller picture of an organization's practices regarding the collection, use, sharing, disclosure and protection of personally identifiable information. Having to provide a comprehensive policy statement promotes data governance and accountability, requiring an organization to consider its data practices and then to ensure that its policies are complied with internally. In addition, like other transparency measures, a privacy policy that must be made public can serve as a catalyst, stimulating changes in practice. Comprehensive privacy policies also inform policy makers and researchers, whose findings often reach the general public through the media. And, as discussed below, a comprehensive privacy policy may be required by law.

California Online Privacy Protection Act

The California Online Privacy Protection Act of 2003 (CalOPPA), the first law in the nation with a broad requirement for privacy policies, is one of California's privacy landmarks. The Act applies to operators of commercial web sites and online services that collect personally identifiable information about Californians. It requires them to say what they do and do what they say—to conspicuously post a privacy policy and to comply with the terms of the policy.

CalOPPA was intended to "help foster the continued growth of the Internet economy . . . by allowing individuals to rely on a privacy policy posted online." The Act's author went on to say that the law's meaningful privacy protections and accessible remedies would help to reassure consumers who were reluctant to do business online.[14]

As originally enacted, the law imposed requirements for what must be included in a privacy policy:

- Categories of personally identifiable information collected through the site or service about users or visitors,
- Categories of third parties with whom the operator may share the personally identifiable information,
- Description of process for a user or visitor to review and request changes to his or her personally identifiable information collected through the site or service, if the operator maintains such a process,
- Description of process for notifying users and visitors of material changes to the privacy policy, and
- Effective date of the privacy policy.

The law defines key terms, including "conspicuously post," "consumer" and "operator." It does not define "online service," although the Attorney General has stated that a mobile application is one type of online service.[15]

"Personally identifiable information" is defined broadly as information about a consumer collected online and maintained by the operator in an accessible form. The types of information considered personally identifiable include the following:

- A first and last name.
- A home or other physical address, including street name and name of a city or town.
- An e-mail address.
- A telephone number.
- A social security number.
- Any other identifier that permits the physical or online contacting of a specific individual.
- 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.

It should be noted that the last two types listed above can be understood to include information that is collected passively by the site or service, such as a device identifier or geo-location data.

The law provides an operator with a 30-day grace period to post a policy after being notified of failure to do so. An operator subject to the law is in violation for failing to comply with the legal requirements for the policy or with the provisions of its policy either knowingly and willfully or negligently and materially.

Online Tracking

Since CalOPPA took effect in 2004, online commerce has burgeoned, and evolving technology and new business practices have raised new privacy concerns. One practice that raises privacy concerns is online tracking, described by the FTC as the collection of data about an individual's Internet activity used to deliver targeted advertisements and for other purposes.[16] In the age of mobile computing, similar tracking is performed on mobile devices by monitoring individuals' use of different apps and features.

In response to privacy concerns, the FTC staff in 2010 proposed a Do Not Track (DNT) browser signal as a uniform and comprehensive way for consumers to choose whether to allow the collection and use of data regarding their online searching and browsing activities.[17] The Commission noted in its 2012 final report that a number of browser vendors had announced that their latest versions permitted consumers "to instruct websites not to track their activities across websites."[18] In a 2012 paper on consumer privacy, the White House noted that "privacy-enhancing technologies such as the 'Do Not Track' mechanism allow consumers to exercise some control over how third parties use personal data or whether they receive it at all."[19] By 2013, the major browser companies had all implemented a DNT mechanism in their browsers.[20] In May 2014, the White House once again commented that consumers "have a valid interest in 'Do Not Track' tools that help them control when and how their data is collected."[21]

There is no legal requirement for how operators of web sites or online services must respond to a browser's DNT signal. The World Wide Web Consortium (W3C), which facilitates collaborative

efforts to develop web standards, created a Tracking Protection Working Group, which has been working since 2011 to develop standards for the technology and meaning of Do Not Track. As of the end of 2013, the W3C group had not agreed upon what an operator or an advertising network should do when they receive a DNT browser header.[22]

AB 370 of 2013: Tracking Transparency

In 2013, the California Legislature passed AB 370, a "tracking transparency" law that amends CalOPPA by adding disclosures about online tracking to the requirements for a privacy policy. The new provisions do not prohibit online tracking, nor do they depend on a standard for how an operator *should* respond to a DNT browser signal or to any mechanism that automatically communicates a consumer's choice not to be tracked. In the words of the author, the law is intended to "increase consumer awareness of the practice of online tracking by websites and online services, such as mobile apps. AB 370 will allow consumers to learn from a website's privacy policy whether or not that website honors a Do Not Track signal. This will allow the consumer to make an informed decision about their use of the website or service."[23]

The law requires two new disclosures in the privacy policy of an operator of a web site or online service subject to CalOPPA:

> (1) the operator's response to a browser DNT signal or to "other mechanisms,"[24] and
>
> (2) the possible presence of other parties conducting online tracking on the operator's site or service.[25]

The "other mechanisms" in the first disclosure requirement can be understood to refer to any technology that, like a Do Not Track browser signal, provides consumers the ability to exercise choice about the collection of their personally identifiable information over time and across third-party web sites or online services. An operator must make the first disclosure only if the operator engages in the collection of personally identifiable information about a consumer's online activities over time and across third-party web sites or online services.

Another provision allows for an alternative way to comply with the first disclosure requirement. The alternative is to provide a "clear and conspicuous" link in the operator's privacy policy to a "program or protocol" that offers consumers a choice about online tracking.[26] The linked location must contain a description of the program or protocol and must describe the effects of the program on consumers who participate in it.

RECOMMENDATIONS

A statement of your general Privacy Policy should provide a comprehensive overview of your practices regarding the collection, use, sharing and protection of personally identifiable information. It should, at a minimum, comply with legal requirements for such policies. The following recommendations are offered as suggestions to make your general Privacy Policy statement more effective and meaningful than a policy that simply meets minimum legal requirements.

SCOPE OF POLICY

Explain the scope of the Privacy Policy, such as whether it covers just your online data collection and use practices or both your online and offline practices.

Clearly indicate what entities the Privacy Policy covers, such as subsidiaries or affiliates.

AVAILABILITY

Make the policy recognizable by giving it a descriptive title.

Make the policy conspicuously available to users and potential users of your web site or online service.[27]

In the case of a web site:
Use a conspicuous link on your homepage 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.[28]

Put a conspicuous “privacy” link on every web page where personal information is collected.

Format the policy so that it can be printed as a separate document.

In the case of an online service, such as a mobile application:
Post or link to the policy on the application’s platform page, so that users can review the policy before downloading the application.

Link to the policy within the application (for example, from the application configuration, “About,” “Information” or settings page).[29]

READABILITY

Use plain, straightforward language. Avoid technical or legal jargon.[30]

Use short sentences. Use the active voice.

Use titles and headers to identify key parts of the policy.

Consider providing your policy in languages other than English.

Use a format that makes the policy readable, including on smaller screens, such as on a mobile device.

- One such format is a layered format that highlights the most relevant privacy issues.[31]
- Graphics or icons can help users easily recognize privacy practices and settings.

DATA COLLECTION

Describe how you collect personally identifiable information.

- If you collect personally identifiable information on users or visitors from other sources, describe how you do so.
- If you collect personally identifiable information through technologies such as cookies or web beacons, describe how you do so.

Describe the kind of personally identifiable information you collect about users and visitors.

- Be reasonably specific in describing the kind of personal information you collect.
- At a minimum, list the categories of personal information that you collect from users and visitors.[32]
- If you collect personally identifiable information from children under the age of 13, you may have additional obligations under federal law. Consult the FTC's guidance on the Children's Online Privacy Protection Act before collecting any such information.[33]

ONLINE TRACKING/DO NOT TRACK

The practice of online tracking—collecting personally identifiable information about consumers as they move across different web sites or online services over time—is invisible to consumers. Consumers whose browsers send a Do Not Track (DNT) signal cannot easily determine how a site or service responds to the signal. Providing a description of your site or service's online tracking practices, and of the possible presence of other parties that may be tracking consumers, can help to make this invisible practice more visible.

Make it easy for a consumer to find the section of your policy that relates to online tracking.

- Clearly identify the section in which you describe your specific policy regarding online tracking or how you respond to consumers' DNT signals. Use a header, for example "How We Respond to Do Not Track Signals," "Online Tracking" or "California Do Not Track Disclosures."

Describe how you respond to a browser's DNT signal or to another such mechanism.[34]

- Describing your response in your privacy policy statement is preferable to simply providing a link to a related "program or protocol" (hereinafter referred to as a "program") because it provides greater transparency to consumers.

  Questions to consider in describing your response:
  Do you treat consumers whose browsers send a DNT signal differently from those without one?

  Do you collect personally identifiable information about a consumer's browsing activities over time and across third-party web sites or online services if you receive a DNT signal?

  If you do continue to collect personally identifiable information about consumers with a DNT signal as they move across other sites or services, describe your uses of the information.

ONLINE TRACKING/DO NOT TRACK

If you decide not to describe your response to a DNT signal or to another mechanism, provide a clear and conspicuous link in your privacy policy statement to a program that offers consumers a choice about online tracking.[35]

- Provide the link in addition to identifying the program with a brief, general description of what it does.

  Questions to consider in providing a link to a program:
  Do you comply with the program? (Your answer should be, "Yes." Say so in your privacy policy.)

  Does the page to which you link contain a clear statement about the program's effects on the consumer, i.e., whether participation results in stopping the collection of a consumer's personally identifiable information across web sites or online services over time?

  Does the page to which you link make it clear what a consumer must do to exercise the choice offered by the program?

Disclose the presence of other parties that collect personally identifiable information on your site or service, if any are present.[36]

- State whether other parties are or may be conducting online tracking of consumers or visitors while they are on your site or service.

  In developing your statement on other parties, consider the following issues:
  Are only approved third parties on your site or service collecting personally identifiable information from consumers who use or visit it?

  How would you verify that authorized third parties are not bringing unauthorized parties to your site or service to collect personally identifiable information?

  Can you ensure that authorized third-party trackers comply with your Do Not Track policy? If not, disclose how they might diverge from your policy.

- Confirm your tracking practices with those responsible for your site's or service's operations to ensure that your practices correspond to what you say in your policy.

DATA USE AND SHARING

Explain how you use and share personally identifiable information.

- Explain the uses of personally identifiable information beyond what is necessary for fulfilling a customer transaction or for the basic functionality of an online service.
- Explain your practices regarding the sharing of personally identifiable information with other entities, including affiliates and marketing partners.
- At a minimum, list the different types or categories of companies with which you share customer personal information.[37]
- Whenever possible, provide a link to the privacy policies of third parties with whom you share personally identifiable information.
- Provide the retention period for each type or category of personally identifiable information collected.

INDIVIDUAL CHOICE AND ACCESS

Describe the choices a consumer has regarding the collection, use, and sharing of his or her personal information.

- Provide clear instructions on how individuals can exercise those choices.
- Respect your customers' preferences by keeping records of preferences and ensuring that they are always honored.
- Implement customer preferences within a reasonable time period.

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.[38]
- Before providing customers access to their personal information, be sure to properly verify identity and authenticate any access right, particularly those 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.

SECURITY SAFEGUARDS

Explain how you protect your customers' personal information from unauthorized or illegal access, modification, use or destruction.

- 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.

EFFECTIVE DATE

Give the effective date of your Privacy Policy.[39]

- Use good version control procedures to ensure that your Privacy Policy is uniform throughout the organization.
- Explain how you will notify customers about material changes to your Privacy Policy.[40]
- Do not rely on merely changing the Privacy Policy on your web site or online service as the exclusive means of notifying customers of material changes in your uses or sharing of personal information.

ACCOUNTABILITY

Tell your customers whom they can contact with questions or concerns about your privacy policies and practices.

Give at minimum 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 a copy of your company's published Privacy Policy.

APPENDIX

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 22577. 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.

(5) Disclose how the operator responds to Web browser "do not track" signals or other mechanisms that provide consumers the ability to exercise choice regarding the collection of personally identifiable information about an individual consumer's online activities over time and across third-party Web sites or online services, if the operator engages in that collection.

(6) Disclose whether other parties may collect personally identifiable information about an individual consumer's online activities over time and across different Web sites when a consumer uses the operator's Web site or service.

(7) An operator may satisfy the requirement of paragraph (5) by providing a clear and conspicuous hyperlink in the operator's privacy policy to an online location containing a description, including the effects, of any program or protocol the operator follows that offers the consumer that choice.

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 home page 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 home page 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 home page 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.

NOTES

[1] Organisation for Economic Cooperation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (2013), available at www.oecd.org.

[2] Evan Hendricks, *Credit Scores and Credit Reports* (2004).

[3] Privacy Act of 1974, 5 U.S.C. § 552a.

[4] Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936; Financial Services Modernization Act of 1999, 15 U.S.C. §§ 6801-6809; Children's Online Privacy Protection Act of 1998 (COPPA), 15 U.S.C. §§ 6501-6506.

[5] Cal. Bus. & Prof. Code §§ 22575-22579.

[6] See Ponemon Institute, *2008 Privacy Trust Study for Retail Banking* (2008), available at www.ponemon.org.

[7] See Mark A. Graber, Donna M. D'Alessandro & Jill Johnson-West, *Reading level of privacy policies on internet health Web sites*, 51 J. Fam. Pract. 642 (2002); Irene Pollach, *What's wrong with online privacy policies?*, 50 Commun. ACM 103 (2007).

[8] See Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 ISJLP 543 (2008); George R. Milne & Mary J. Culnan, *Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices*, 18 J. Interactive Marketing 15 (2004).

[9] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (2012), available at www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers.

[10] The White House first proposed the Consumer Privacy Bill of Rights in *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (2012) and continued to urge advancing it in *Big Data: Seizing Opportunities, Preserving Values* (May 2014).

[11] On layered notices, see the Center for Information Policy Leadership, *Ten steps to develop a multilayered privacy notice* (2007), available at www.informationpolicycentre.com. On a privacy nutrition label format, see Patrick Gage Kelley, Joanna Bresee, Lorrie Faith Cranor & Robert W. Reeder, *A "Nutrition Label" for Privacy*, Proceedings of the 5th Symposium on Usable Privacy and Security (SOUPS), 2009, available at cups.cs.cmu.edu/privacyLabel.

[12] See *supra* note 10.

[13] California Attorney General, *Privacy on the Go: Recommendations for the Mobile Ecosystem* (2013), available at www.oag.ca.gov/privacy; National Telecommunications and Information Administration, *Short Form Notice Code of Conduct to Promote Transparency in Mobile App Practices* (2013), available at www.ntia.doc.gov/other-publication/2013/privacy-multistakeholder-process-mobile-application-transparency.

[14] Cal. Bus. & Prof. Code §§ 22575-22579. For the author's statement, see *Personally Identifiable Information: Disclosure of Online Privacy Policy: Hearing on AB 68 (Simitian) Before the A. Comm. on the Judiciary*, 2003-2004 Reg. Sess. (Apr. 22, 2003), available at www.leginfo.ca.gov/.

[15] See Press Release, California Attorney General, *Attorney General Kamala D. Harris Secures Global Agreement to Strengthen Privacy Protections for Users of Mobile Applications* (Feb. 22, 2012), available at www.oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-secures-global-agreement-strengthen-privacy. Many of the terms used in CalOPPA, including "online service," were based on terminology in the federal Children's Online Privacy Protection Act (COPPA). The FTC, in its publication *Complying with COPPA: Frequently Asked Questions* (2013), names mobile apps as included in online services in the answer to Question 2 available at www.business.ftc.gov/documents/Complying-with-COPPA-Frequently-Asked-Questions#General Questions.

[16] Federal Trade Commission, *The Do Not Track Option: Giving Consumers a Choice*, www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/do-not-track.

[17] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Business and Policymakers, Preliminary Staff Report* (2010), available at www.ftc.gov/news-events/press-releases/2010/12/ftc-staff-issues-privacy-report-offers-framework-consumers. The Do Not Track header was originally proposed in 2009 by researchers Christopher Soghoian, Sid Stamm and Dan Kaminsky. See Christopher Soghoian, *The History of the Do Not Track Header*, Slight Paranoia (Jan. 21, 2011), paranoia.dubfire.net/2011/01/history-of-do-not-track-header.html.

[18] See *supra* note 17.

[19] White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (2012), available at www.whitehouse.gov/sites/default/files/privacy-final.pdf.

[20] The Future of Privacy Forum's *All About Do Not Track (DNT)* web page includes information on how the different browsers implement the function, as well as other information on Do Not Track. See *All About Do Not Track (DNT)*, allaboutdnt.com (last visited Feb. 12, 2014).

[21] White House, *Big Data: Seizing Opportunities, Preserving Values* (2014), available at www.whitehouse.gov.

[22] For more information on the W3C Tracking Protection Working Group, see *Tracking Protection Working Group*, W3C, www.w3.org/2011/tracking-protection (last visited Feb. 12, 2014).

[23] See *Consumers: Online Tracking: Hearing on AB 370 (Muratsuchi) Before S. Comm. on the Judiciary*, 2013-2014 Reg. Sess. (June, 18, 2013), available at leginfo.legislature.ca.gov.

[24] Cal. Bus. & Prof. Code § 22575(b)(5).

[25] Id. § 22575(b)(6).

[26] Id. § 22575(b)(7). Note that the term used here, "program or protocol," is not the same as the term used in subdivision 5, "mechanism."

[27] Id. § 22575(a).

[28] Id. § 22577(b)(3).

[29] Because online services, such as mobile applications, may have varied and smaller user interfaces than web sites, CalOPPA permits more flexibility in how operators may conspicuously post their privacy policy, namely "any other reasonably accessible means of making the privacy policy available for consumers of the online service." See Id. §22577(b)(5).

[30] 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.

[31] See, e.g., National Telecommunications and Information Administration, *Short Form Notice Code of Conduct to Promote Transparency in Mobile App Practices* (2013), *supra* note 13.

[32] Cal. Bus. & Prof. Code § 22575(b)(1).

[33] Federal Trade Commission, *Complying with COPPA: Frequently Asked Questions, A Guide for Business and Parents and Small Entity Compliance Guide* (revised July 2013), www.business.ftc.gov/documents/Complying-with-COPPA-Frequently-Asked-Questions.

[34] Cal. Bus. & Prof. Code § 22575(b)(5).

[35] Id. § 22575(b)(7).

[36] Id. § 22575(b)(6).

[37] Id. § 22575(b)(1).

[38] Id. § 22575(b)(2).

[39] Id. § 22575(b)(4).

[40] Id. § 22575(b)(3).

California Department of Justice
Privacy Enforcement and Protection Unit

www.oag.ca.gov/privacy