GIBBS GIDEN ATTORNEYS AT LAW
LOCHER TURNER SENET & WITTBRODT LLP

eINSIGHT

New California Privacy Laws Affect Online Web and Mobile Nationwide: Attorney General Offers Guidance for Web Companies and Mobile Apps in California and Beyond

By Luke N. Eaton
and
Matthew Robinson

June 9, 2014

Amidst the increasing public frustration over the use and leaking of private personally identifying information ("PII") by government and private entities, California Attorney General Kamala Harris recently issued guidelines[1] to help companies comply with the California Online Privacy Protection Act of 2003 ("CalOPPA").[2]

Kamala Harris has been particularly active in this area of Online Privacy since she took the California Attorney General office in 2011. The recent amendment, effective January 1, 2014, is the first major activity on CalOPPA since it went into effect in 2004. Harris is also making special efforts to enforce CalOPPA, which does not itself have an enforcement provision, under California's Unfair Competition Law, which permits penalties of up to $2,500 per violation.[3] In 2013, Harris brought suit against Delta Airlines to enforce these penalties for violations to CalOPPA, but the suit was dismissed on other grounds.[4] Thus, while it generally remains to be seen how the courts will interpret CalOPPA and this method of enforcement, it is clear that Harris is determined to take action in order to enforce the CalOPPA provisions.

[1] https://oag.ca.gov/sites/all/files/agweb/pdfs/cybersecurity/making_your_privacy_practices_public.pdf.

[2] Cal. Bus. & Prof. Code §§ 22575-22579. http://oag.ca.gov/privacy/COPPA.

[3] Cal. Bus. & Prof. Code §17206(a).

[4] http://www.law360.com/privacy/articles/388249?nl_pk=921346cf-b42b-4679-8d74-5a108e64feae&utm_source=newsletter&utm_medium=email&utm_campaign=privacy.

With its recent amendment, the CalOPPA impacts all individuals and companies considered to be operators[5] that collect PII[6] of California residents, which in the "borderless world of online commerce" may extend to even individuals living and companies formed in other jurisdictions.[7] Any company or individual who may be impacted should seriously consider evaluating whether their current privacy policy complies with all of the new CalOPPA requirements in order to avoid potential fines of up to $2,500 per violation with respect to each individual consumer using their Web site or service (e.g., mobile application).[8]

The aggregate of each potential penalty assessed could grow exponentially and very quickly. The CalOPPA does provide each operator with a 30-day grace period to post a compliant privacy policy after being notified that its current policy fails to comply with CalOPPA requirements.[9] However, every potential operator should take action immediately in order to avoid being subject to this effective 30-day deadline with its consequence of potential, substantial penalties.

Brief Background of CalOPPA

In addition to protecting consumer constitutional rights to privacy, the purpose of CalOPPA is to foster the continued growth of the Internet economy by increasing consumer trust through transparency.[10] CalOPPA requires operators to conspicuously post a privacy policy and to comply with the terms of the policy.[11]

Additionally, CalOPPA requires that an operator's privacy policy include specific disclosures, such as an explanation of the categories of PII collected by the Web site or service (e.g., mobile application) about consumers and the types of third parties with whom the operator may share the PII.[12] The amendment, effective January 1, 2014, adds two new disclosures to the list of

---

[5] Defined by Cal. Bus. & Prof. Code §22577(c) as "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."

[6] The term "personally identifiable information" as defined by CalOPPA means "individually identifiable 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: (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; and (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. 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."

[7] Kamala Harris, *Making Your Privacy Practices Public*, 1, 3 (May 21, 2014), https://oag.ca.gov/sites/all/files/agweb/pdfs/cybersecurity/making_your_privacy_practices_public.pdf.

[8] Cal. Bus. & Prof. Code §17206(a).

[9] Cal. Bus. & Prof. Code §22575(a).

[10] 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/.

[11] Cal. Bus. & Prof. Code §22575(a).

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

required disclosures to be included in an operator's privacy policy. These two new disclosures include: (1) how the operator will respond to a consumer's Do-Not-Track ("DNT") signal or other similar consumer choice regarding the collection of his or her PII, and (2) the possible presence of other third parties conducting online tracking on the operator's Web site or service.[13]

The Attorney General's Guidelines

On May 21, 2014, the California Attorney General issued guidelines to help operators comply with CalOPPA, as amended. These guidelines do not have the force of law, and they in fact may exceed the protection required by CalOPPA. Nevertheless, the guidelines are intended to "encourage companies and other organizations to provide meaningful privacy policy statements."[14] If you or your Web business may be considered an operator, please consider implementing these guidelines to your privacy policy.

The following items highlight the Attorney General recommendations as to what information should be included in your privacy policy and how it should be displayed:

Availability:

- Make your privacy policy conspicuously available to consumers/potential consumers of your Web site or online service by including a link with the word "privacy" in text that is larger than the surrounding text, contrasted in a different color, or showcased by symbols that call attention to it.
- In the case of an online service, such as a mobile application, post or link to your privacy policy on the application's platform page, so that consumers can review the policy before downloading the application. Also, link to the policy within the application.

Readability:

- Use plain, straightforward language in your privacy policy, avoiding technical or legal jargon. Use preferably short sentences in the active voice, and consider providing your policy in languages other than English.
- Use titles, headers, and a general format (e.g., a layered format) that helps identify key parts of your privacy policy and the most relevant privacy issues.

Online Tracking/Do Not Track:

- Specifically label the section of your privacy policy that relates to online tracking and the section that relates to how you respond to consumers' DNT signals in order to make it easy for consumers to find each of them. Use a header, such as "How We Respond to Do Not Track Signals," "Online Tracking" or "California Do Not Track Disclosures."
- You must describe how you respond to a consumer's Web browser DNT signal or to another such mechanism. Your description may be accessible by providing a clear and

[13] Cal. Bus. & Prof. Code §22575(b)(5) and (6).

[14] Kamala Harris, *Making Your Privacy Practices Public*, 1, 3 (May 21, 2014), https://oag.ca.gov/sites/all/files/agweb/pdfs/cybersecurity/making_your_privacy_practices_public.pdf.

conspicuous hyperlink in your privacy policy. However, it is preferable that you describe your response to DNT signals or similar mechanisms directly in your privacy policy.

Third Party Online Tracking/Third Party Do Not Track:

- Disclose whether third parties are or may be conducting online tracking of consumers or visitors while they are on your Web site or service.
- In determining what information to include in this disclosure, consider (a) whether only approved third parties are on your site or service collecting PII from consumers; (b) how you would verify that authorized third parties are not bringing unauthorized parties to your site or service to collect PII from consumers; and (c) whether you can ensure that authorized third-party trackers comply with your DNT policy.

Data Use And Sharing:

- Explain the uses of PII beyond what is necessary for fulfilling a consumer transaction or basic functionality of an online service.
- Identify the different types or categories of consumer PII that you collect and the different types or categories of companies with which you share consumer PII.
- Whenever possible, provide a link to the privacy policies of third parties with whom you share consumer PII.
- State the retention period for each type or category of PII collected from consumers.

Individual Choice and Access:

- Describe the choices a consumer has regarding the collection, use, and sharing of his or her personal information, and provide clear instructions on how consumers can exercise those choices.
- Implement consumer preferences within a reasonable time period, and keep records of preferences to ensure that they are always honored.
- If you maintain a process where a consumer may review and request a change to any of his or her PII that is collected through the Web site or service, describe that process.

Security Safeguards and Accountability:

- Explain how you protect your consumers' personal information from unauthorized or illegal access, modification, use or destruction (e.g., when information is in your care and when information is in the care of third parties).
- Give the effective date of your private policy, and explain how you will notify consumers about material changes to your privacy policy.
- Provide a title and e-mail or postal address of a company official whom your consumers can contact with questions or concerns about your privacy policy and practices.

Conclusion

As mentioned above, CalOPPA defines an operator as any individual or entity who "collects and maintains personally identifiable information from a consumer residing in California." For this reason, the CalOPPA laws are applicable to any online business collecting such information whether that business operates primarily in California or in any other jurisdiction. In response to this legislation, any Web business that could potentially be defined as an operator should ensure

that their privacy policy is compliant with CalOPPA. Even as we wait to see how the courts interpret the law and its enforcement, it is clear that the Attorney General will continue enforcement efforts, and the potential for a $2,500 fine per violation of CalOPPA should have your immediate attention.

Additionally, while California's CalOPPA amendment, specifically regarding Do-Not-Track signals, is the first of its kind by either state or Federal legislation, it is likely not the last. Interest is growing in this area. The White House commented on the subject as recently as in May 2014, stating that consumers "have a valid interest in 'Do Not Track' tools that help them control when and how their data is collected."[15]

Currently, there are no Federal or other similar state laws in this area of Online Privacy. However, it is likely that there will be future similar Federal and/or state legislation that will, like CalOPPA, impact Web businesses nationwide. And because the California Attorney General guidelines will likely serve as the standard for all future legislation on the subject, it would be wise to begin implementing these guidelines into your privacy policy now.

California is once again leading the way in legislating to respond to issues in Online Privacy, and every online business inside and outside of California may potentially be affected. At this juncture, it would be prudent for Web companies nationwide to review the guidelines in connection with their current privacy policies to ensure compliance with CalOPPA and help prepare for potential additional state or Federal legislation in the future.

For more information contact
Luke N. Eaton, Esq.
and
Matthew Robinson, Esq.
Gibbs Giden Locher Turner Senet & Wittbrodt LLP
1880 Century Park East, 12th Floor
Los Angeles, California 90067
Phone: (310) 552-3400
email: lneaton@ggltsw.com
email: **mrobinson@ggltsw.com**

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