November 12, 2014

Privacy Policies 2.0: Making Disclosures More Meaningful

By Leonard A. Ferber, Co-Head, Technology Practice

Website privacy policies are a ubiquitous fact of web life, intended to allow users to easily understand the personal information being collected by a website and how that site uses and shares that information. Over time, however, privacy policies have gotten longer, denser and exceedingly complex—a seeming embodiment of the "Go Big or Go Home" ethos. Consequently, privacy policies have become less useful, and few consumers understand or even try to read them. However, with the publication earlier this year of *Making Your Privacy Practices Public* (the Guide), the Attorney General of California (CAG) tackled this issue head-on, seeking to reverse the trend and make privacy policies more meaningful.

The State of California has long been the leader in promoting privacy on the Web. With the California Online Privacy Protection Act of 2003 (CalOPPA), California was the first state to require websites to post privacy policies, and later confirmed that this obligation applied to mobile sites as well. The CAG formed a Privacy Enforcement and Protection Unit to educate consumers, provide guidance to businesses and enforce both federal and state privacy laws. Most recently, the California Legislature passed AB 370, which amended CalOPPA to require disclosures regarding online tracking. While, on their face, the privacy laws of California apply only to companies collecting personally identifiable information of California residents, the CAG's aggressive focus on privacy, coupled with, as the Guide notes, California's "economic importance and the borderless world of online commerce," makes California law required reading for all website operators.

The Guide provides a full set of recommendations for drafting privacy policies, and much of what it presents are common sense explanations of the text of CalOPPA. The real advancement fostered by the Guide, however, is two-fold. First, it provides guidance on the newly required disclosure of online tracking under CalOPPA. Second, and more importantly, the CAG used the Guide to focus on **how** to make privacy policies more meaningful to users. This focus ushers in, what I call, "Privacy Policies 2.0"—a realization that in drafting privacy policies, much like a meal at a 4-Star restaurant, presentation is just as important as substance.

Disclosure of Online Tracking Activities

The issue of "online tracking" has generated much confusion. The term refers not to the relatively harmless tracking of a site user as he or she moves around a particular site, but rather to the collection of data over time regarding an individual's Internet activity as that person moves from site to site. Such information is used to deliver targeted advertisements. Such tracking is seen as particularly invasive of one's privacy and, as a result, most web browsers allow users to set their preferences such that the browser can send a signal to sites that the user does not want to be tracked. While industry groups

For more information, please contact any of the following members of Katten's **Technology practice**.

Leonard Ferber
+1.312.902.5679
leonard.ferber@kattenlaw.com

Tanya Curtis
+1.312.902.5593
tanya.curtis@kattenlaw.com

Doron Goldstein
+1.212.940.8840
doron.goldstein@kattenlaw.com

have proposed "do not track" (DNT) rules or standards for the technology and meaning of DNT, no consensus has been reached and currently there is no legal requirement for how websites or advertising networks must respond to a DNT signal.

California's AB 370 sought to fill the void by requiring website operators that collect personally identifiable information from citizens of California to make two disclosures regarding online tracking:

(1) 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 websites or online services, if the operator engages in that collection; and

(2) disclose whether other parties may collect personally identifiable information about an individual consumer's online activities over time and across different websites when a consumer uses the operator's website or service.

While it is clear that the amendment does not prohibit online tracking or mandate how an operator should respond to a DNT browser signal, the wording of the required disclosures is less clear. The CAG has now provided clarification. As for the first disclosure requirement, the Guide makes clear that an operator must disclose the operator's response to a browser DNT signal, but **only if** the operator engages in online tracking. As for the second requirement, disclosure should be made as to "the possible presence of other parties conducting online tracking on the operator's site or service."

Additional recommendations for disclosure beyond that required by the statute are provided as well. For example, where a site responds to a DNT signal, the CAG encourages disclosing whether (1) consumers whose browsers send a DNT signal are treated differently from those whose browsers do not and (2) personally identifiable information about a consumer's browsing activities across the Internet is still collected notwithstanding that a DNT signal is received.

The CAG recognizes that many companies do not fully understand the scope of third-party data collection on their site. This may result from a company's marketing function contracting with outside parties without involvement from its technology or legal departments or because authorized third-party trackers may bring unauthorized parties to the site. The Guide therefore suggests that operators "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."

Privacy Policies 2.0 – A Focus on Presentation

Realizing that "[m]any privacy policies . . . are overly long and difficult to read without offering meaningful choices to consumers" and that "[d]issatisfaction with the effectiveness of privacy policy statements has grown over time," the CAG acknowledges that the purpose of the Guide is to make privacy policies more "meaningful." Accordingly, the CAG focuses as much on how a privacy policy is presented as on its substance. Perhaps channeling an inner high school English teacher, the CAG provides the following recommendations for promoting "readability":

- Use plain, straightforward language. Avoid technical or legal jargon.
- Use short sentences. Use the active voice.
- Use titles and headers to identify key parts of the policy. For example, it is suggested that operators should make it easy to find the section describing the online tracking policy by labeling it, for example: "How We Respond to Do Not Track Signals," "Online Tracking" or "California Do Not Track Disclosures."
- Consider providing your policy in languages other than English.

Formatting is also addressed with the following suggestions:

- Use a layered format that highlights the most relevant privacy issues.
- Use graphics or icons to help users easily recognize privacy practices and settings.
- Whenever possible, provide a link to the privacy policies of third parties with whom you share personally identifiable information.

As a result of these suggestions, it appears that the old adage for privacy policies to "say what you do and do what you say," may not be enough anymore. Now the regulators will increasingly look at how you say it.

Balancing Substance vs. Form

Still, there remains a tension between the desire for a readable, easily understandable privacy policy, on the one hand, and the need to provide complete transparency, on the other. In this regard, it should not go unmentioned that the recent amendment to CalOPPA serves only to *increase* the required disclosures. As the CAG notes:

> "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."

What to do then? The answer is to create two or more notices: a long form and supplemental "simpler, shorter privacy notices to alert consumers to potentially unexpected data practices." As the Guide explains:

> "Rather than describing the full range of data practices, such a [supplemental] 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."

This suggestion is consistent with the "surprise minimization approach" to privacy notices which the CAG first recommended in 2013 in its publication *"Privacy on the Go: Recommendations for the Mobile Ecosystem."* Specifically, an operator would highlight in shorter special notices the collection of personally identifiable information that users would not likely expect, such as those not necessary for a site's or app's basic functionality (such as fulfilling a customer transaction or the basic functionality of an online service) or particularly sensitive information, such as medical or financial information. This approach seeks to counter the reality than when privacy policies "drone on and on" about non-controversial matters, such as collecting personal information inputted manually by the user or the use of cookies to record usage within a site, consumers fail to take notice of privacy issues they will actually care about.

Conclusion

The Guide is a valuable resource and offers "best practices" for the drafting of privacy policies but they are not, as the CAG admits, regulations, mandates or legal opinions and "in some places offer greater privacy protection than required by existing law." The CAG believes that following the Guide will make privacy policies "more effective and meaningful than a policy that simply meets minimum legal requirements." Still, one does not have to be too paranoid to feel that enforcement efforts will seek compliance with these best practices, leaving to website operators the unenviable task of arguing that the recommendations go beyond the law.

But if the goal is to make privacy policies more meaningful, I believe the lasting value of the Guide will be in ushering in the next generation of Privacy Policies.

Katten

Katten Muchin Rosenman LLP www.kattenlaw.com

AUSTIN | CENTURY CITY | CHARLOTTE | CHICAGO | HOUSTON | IRVING | LONDON | LOS ANGELES | NEW YORK | ORANGE COUNTY | SAN FRANCISCO BAY AREA | SHANGHAI | WASHINGTON, DC

Attorney advertising. Published as a source of information only. The material contained herein is not to be construed as legal advice or opinion.

©2014 Katten Muchin Rosenman LLP. All rights reserved.

Katten Muchin Rosenman LLP is an Illinois limited liability partnership including professional corporations that has elected to be governed by the Illinois Uniform Partnership Act (1997). London: Katten Muchin Rosenman UK LLP.

11/10/14