wiley

NEWSLETTER

Has Your Company Reviewed Its Privacy Policy Lately?

April 2014

An inaccurate privacy policy runs a risk of being deemed a misleading or deceptive trade practice under federal or state consumer protection laws. Even a policy that accurately described a company's practices a few years ago may no longer do so because business practices change. And, in any event, recent changes in laws and regulations mean that most company privacy policies may no longer meet legal requirements.

Website Privacy Policies and the CalOPPA

Since 2004, the California Online Privacy Protection Act (CalOPPA) has required commercial websites or online services with users residing in California—which means nearly every commercial website operated in the United States and potentially many others—to "conspicuously post" an online privacy policy, labelled "privacy." CalOPPA requires that the privacy policy address certain specified topics, among the most important of which is that a company's privacy policy disclose what "personally identifiable information" (PII) is collected by its website and with whom it is shared.

Consider when the privacy policy was last updated (this should be readily discernable, because, by law, the posted policy must state its effective date). Think about how the site has changed since that date. Have features been added or subtracted? Is the site now collecting any types of data that it was not collecting at the time the current policy was drafted? Has the business made any changes in how it uses, shares, or saves the personal information that it collects? Does the company share customers' personal information—as defined by CalOPPA or other laws—with third parties? Has anything changed about how the website uses advertising networks and analytics companies? How does the current privacy policy address the use of "share" buttons and similar plug-ins that inherently share personal information, at least under some definitions?

Moving off of the traditional website, does the company now offer a mobile application? Is it active on Twitter or Facebook? Policies that may have described a website's operations several years ago may have little relationship to a company's mobile app or social media presence.

Beyond these business questions, recent amendments to CalOPPA require additional disclosures. Websites now must disclose how they, and any third-parties that provide services to that site, respond to "do not track" signals from browsers. Another new provision requires websites to disclose whether third parties collect PII on

the operator's website over time and across other sites, which enables the practice known as behavioral targeting.

In addition, California also recently enacted an "eraser" law that will empower registered users under the age of 18 (significantly higher than the federal COPPA standard of 13) of a site "predominantly comprised of minors" to direct websites to remove, or request the removal of, content that the youth has posted. This law will take effect on January 1, 2015, so companies should begin planning how they will come into compliance.

While reviewing the effect of these new laws on a company's privacy policy, it might also be desirable to review the website's compliance with other California laws of somewhat older vintage, including the "Shine the Light" law and the data breach notification law (which itself recently was amended to apply to more data). Both of these laws encourage businesses to have plans in place to address the situations where notice may be required, which may enable businesses to avoid more costly steps in the event the laws are triggered.

Although California's CalOPPA in practice provides what in effect is a national baseline for privacy policies, numerous other state laws, federal laws, compilations of industry best practices, and consumer protection laws impose still other obligations on businesses and their privacy policies. Websites increasingly should be mindful of whether information about people that they may make available constitutes "credit reports" under the federal Fair Credit Reporting Act. And they also should be aware of the Federal Trade Commission's (FTC) increasingly extensive history of bringing enforcement actions on privacy issues.

Mobile Apps

Seemingly everyone today makes available a smartphone mobile application. What information does your company's app collect? Does it copy the user's address book and, if so, why? And is that fact disclosed to the user? Where?

Businesses should ensure that their mobile app privacy practices are reflected in a privacy policy, and it is advisable where possible to strive for consistency between their website and mobile app policies. Unless the mobile app has its own, readily available and conspicuous privacy policy, regulators will likely deem, as they have in cases to date, the online privacy policy to apply.

Pursuant to a 2012 agreement between the California Attorney General and the eight leading online app store platforms, the platforms must provide a means by which a prospective user may review the privacy practices of the app before it is downloaded, either through a statement or a hyperlink, if the app makes that available. (Note that the California Attorney General has taken the position that CalOPPA requires apps to have a privacy policy.) Consistent with this, a company should review the accuracy of the disclosures made by the app itself and at the app store platform from which it is available for download. And it should consider whether different versions of its apps collect, use, or share information differently, both by operating system and by iteration of the app.

Both federal and state regulators have brought enforcement actions against mobile app providers for allegedly misleading statements in their privacy policies regarding a mobile app. In recent years, the FTC has brought a number of enforcement actions against app developers and owners. For example, last year the FTC charged Goldenshores Technologies, which offered a flashlight app, for not appropriately disclosing in its privacy policy or end user license agreement that the flashlight app collected geo-location data and shared that information with third parties. In other words, the FTC charged Goldenshores with a material omission for failing to disclose adequately that it collected and shared location data, which the FTC regards as particularly sensitive. (See FTC Acts Against App's Undisclosed Geolocation Dissemination, December 2013 *Privacy In Focus*).

To help companies address privacy issues arising from their mobile apps, a number of industry groups and trade associations have developed codes of conduct or best practices. Once again, the California Attorney General has expressed a view, publishing a set of "Privacy on the Go" recommendations in January 2013. Many industry groups and think tanks have chimed in with recommended best practices as well. All of these are sources of good advice. However, if a company is a member of one of these groups, or has pledged to adhere to a particular code, then it should ensure that it does in fact live up to those recommendations.

In addition, in 2013 a multistakeholder group convened by the National Telecommunications and Information Administration released a draft code of conduct regarding the transparency of privacy practices in mobile apps. That code, which will most directly affect app developers, as they actually write the app software, provides that an app should present, before being downloaded, certain specified information regarding whether certain categories of personal data are collected by the app and, if so, whether those data are shared and with whom.

Children

A company must also evaluate the implications of the FTC's recent revisions to its rule implementing the Children's Online Privacy Protection Act (COPPA). One may think that a site does not collect personal information from children under the age of 13, but there are ways to trip up. One of the more obvious ones is collecting years of birth, which can result in a site being charged with having knowledge of any users under age 13.

Furthermore, in amendments to its regulation implementing COPPA that took effect last July, the FTC broadened the definition of "personal information" that is subject to the prior verifiable parental consent requirement, and expanded the rule to apply both to third-party plug-ins such as the Facebook "Like" button and to third-party advertising networks. The revised regulation also specifically applies to mobile apps. In addition, the revised regulation also has changed how a site aimed "predominantly" at teenagers can confine its COPPA-related obligations to those children who are under 13. (See FTC's New COPPA Rule Expands Children's Online Privacy Obligations, January 2013 *Privacy In Focus*).

Understanding the current COPPA requirements is vital, because many commonplace website and mobile app practices can inadvertently run afoul of the rule. The same rules govern mobile apps used by children, but compliance is more complex due to the smaller screens on smart devices.

Data Security and Breach Notification

Finally, the attention—and lawsuits—relating to the highly-publicized 2013 data security breaches experienced by Target and by Neiman Marcus serve as a pointed reminder of the need to attend to data security throughout a company's operations, both online and offline. What can a business do to guard against similar breaches, what should it do to prepare for one, and what must, can, or should it say in a privacy policy?

More than 45 states now have breach notification laws on the books. However, even if a company's website has changed little, the law has. For example, user names and email addresses were not defined as "personal information" by California's breach notification law until January 1 of this year, although they may meet the definition of personal information under other laws (such as COPPA). This effectively converted a law meant to deter identity theft and financial fraud into a more general data protection statute. This also means that a privacy policy that does not classify email addresses and user names as personal information is out of date.

Reviewing a privacy policy can provide a good opportunity for a company to take steps to address the risks to data security and how to provide notification to consumers in the event of a data security breach. When was the last time your company reviewed the cybersecurity of its website, payment systems, or other electronic systems? Does it have a plan to address cyber-attacks? To address data breaches?

And pay attention to the security features of apps. In late March, the FTC announced that it had entered into consent decrees with two companies, Credit Karma and Fandango, for failing to take reasonable steps to secure their apps. Interestingly, the FTC specifically cited both companies for disabling the SSL certificate validation, which would have verified that the apps' communications were secure, and thereby potentially exposing users' data to hackers and thieves. The consent decrees being entered into in those cases will require the companies to put in place comprehensive security programs to address risks related to the development and management of new and existing products and to protect the security, integrity, and confidentiality of information covered by the order. Under the decrees, the companies will remain subject to independent security audits every other year for the next 20 years. A similar fate could well befall other companies that do not take what the FTC regards as reasonable steps to secure their apps.