ALM
LAW JOURNAL
NEWSLETTERS

# The Murky World of Online Privacy

March 2013
*By David J. Shaw*

The time has long passed when companies of any size, in any industry can take a lax approach to privacy policies. Between California starting to enforce its online privacy law, and the Federal Trade Commission (FTC) making changes to federal regulations regarding the online use of information from children, closer scrutiny than ever is being paid to this issue. And that scrutiny comes with hefty fines and legal implications that can ensnare any company with an online presence or mobile application. This article examines the compliance issues raised by California's Online Privacy Protection Act, and the FTC's recent changes to the federal Children's Online Privacy Protection Act, and what companies must do to ensure they are not in violation.

## California's COPPA

The California Online Privacy Protection Act of 2003 (CA-COPPA), Cal. Bus. & Prof. Code §22575 - 22579 (2004), is now being enforced by the California Attorney General's Office. Violations of CA-COPPA carry a heavy penalty at $2,500 per violation. Especially when pertaining to mobile application downloads, such a hefty fine multiplies quickly. Yet, analysis of company's compliance level, and potential remediation if needed, can be easily achieved while still maintaining cost-consciousness. The key is to understand what is required by CA-COPPA and to review existing policies accordingly, or to immediately implement new policies where necessary.

So, what does California's COPPA require? According to the Act, each commercial website operator that collects personal information about Californians who visit its Web pages must post a distinctive and easily found link to the website's privacy policy. This policy must describe:

1. The types of information gathered;
2. The ways information may be shared with other parties; and
3. The process whereby a user can review and modify his or her personal information.

Finally, the policy must also state the effective date and describe any subsequent changes since the

effective date.

## Does It Apply?

CA-COPPA is far-reaching. Although a California law, it is applicable to anyone who gathers information on people living in California. Presumably, this would be true even if a website owner did not know the person to whom the information applies lives in California. Enforcement by California officials on out-of-state or out-of-country website owners is a challenging issue, but for the potential monetary losses involved (especially given the relatively inexpensive costs of developing a legal privacy policy), it is simply not worth the risk of running a commercial website or having an online commercial application of any kind without a solid privacy policy.

## Types of Information Gathered

Under CA-COPPA, companies must maintain privacy policies which describe the categories of information gathered about Californians. Specifically, the categories must include the following types of "personally identifiable information" when collected and maintained by the company:

1. First and last name;
2. Home or other physical address, including street name and name of a city or town;
3. e-Mail address;
4. Telephone number;
5. Social Security number;
6. Any other identifier that permits the individual to be contacted in person or online; or
7. The combination of any of the foregoing categories.

Ironically, at least some of the foregoing categories may be otherwise publicly available, yet CA-COPPA contains no exemptions from compliance when that is the case. The safest course, then, is to conduct a full review of existing policies and to implement changes where necessary.

## Information Sharing with Other Parties

Privacy policies must also specify which of the above categories of information may be shared with third parties, and must describe the categories of third parties with whom the information is shared. Importantly, CA-COPPA does not prohibit or restrict the sharing of information with third parties. Instead, there simply must be disclosure in the privacy policies about the categories of receiving parties and the information shared.

## User Modification of Personal Information

CA-COPPA further requires privacy policies to describe the process whereby an individual can review, modify and remove his or her personal information. As with the description of categories above, the key to compliance is ensuring a removal and modification process exists and is disclosed. Equally critical is ensuring that internal company practices follow the described process. In other words, if the policy says the company will remove information upon written request, but in practice nothing is ever removed, then CA-COPPA may have been violated nonetheless. To combat this potential disconnection, it is highly recommended that compliance be centralized and adequate training be given to all personnel responsible for compliance.

## Effective Date

The privacy policy must identify the original effective date, subsequent amendment dates and, if amended, a description of the changes made since the original policy was implemented. As a practical matter, this provision requires internal diligence to track revisions as they are made.

## Conspicuous Posting

Finally, the privacy policy must be conspicuously posted. This requires a link to the policy on the company's homepage or first page with significant substance. Since the latter option is undefined in CA-COPPA, caution dictates that a link to the policy simply be placed on the company's main landing page. CA-COPPA is also explicit in its requirements for hyperlinking to the policy. To be compliant, the hyperlink must at least include the word "privacy," be written in capital letters equal to or greater in size than the surrounding text, or be written in larger type than the surrounding text, 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 intent is to ensure an individual's attention is easily drawn to the privacy policy.

## FTC's COPPA

Second, the FTC recently announced new rules under the Federal "Children's Online Privacy Protection Act of 1998" (for purposes of this article, "FTC-COPPA"). The general rule under FTC-COPPA hasn't changed — if a company knowingly collects information from children, or children self-report information and they are in fact minors, then FTC-COPPA applies. The new rules, however, establish the new compliance categories.

## New Provisions

The new FTC compliance categories further complicate an already murky area of law by implementing new subparts of FTC-COPPA by rule and, therefore, new potential pitfalls. Presumably, the intent of the new subparts is to further expand the applicability of FTC-COPPA to companies that have found ways to sidestep the previous rules. But, the danger for kid-oriented companies and their vendors and

suppliers is the risk of heightened enforcement by the FTC for non-compliance. This wouldn't be of great concern if the subparts clearly articulated what is required and of whom — but they don't. Instead, the new subparts are unclear and, therefore, subject kid-oriented companies to heightened scrutiny without being able to accurately predict how to behave in advance to comply. That said, the subparts are as follows:

### *Subpart A: Appeal to 12 and Under*

This provision of FTC-COPPA applies when site/app content appeals to kids 12-and-under. The factors in determining appeal are expanded, but this definition isn't new. It is sufficient for the purposes of this article to understand that child-specific applications have unique requirements, the details of which must be reserved for later discussion.

### *Subpart B: Actual Knowledge of Another Website*

When a service "has actual knowledge that it is collecting personal information directly from users of another website or online service directed to children" this provision applies. The intent is to cover third-party vendors who attempt to reach kids. Even assuming the intent is noble, it remains unclear how to determine whether or not the other website's service is "directed to children."

### *Subpart C*

This provision applies to services "directed" to kids even when they are not targeted as the primary audience. The definition, however, is circular since the rules define "directed" to kids as "targeted" to kids, thus obliterating any meaningful difference.

### *Compliance*

The express compliance requirements of FTC-COPPA are yet more complicated than CA-COPPA. Where applicable (Subparts A, B and C), website operators must:

1. Provide notice to parents;
2. Obtain verifiable parental consent prior to collecting using, or disclosing personal information from children;
3. Keep information collected from children secure; and
4. Prohibits conditioning children's participation in activities on the "collection of more personal information than is reasonably necessary to participate in such activities."

So, the best practical rule is this: If your company collects information identifying users as under 13 years old, or has Web content or applications that might appeal to children, further legal review should be mandatory before "going live."

## Conclusion

Whether governed by CA-COPPA or FTC-COPPA, or simply seeking to implement best corporate practices, implementing sloppy privacy policies is not worth the potential risks of non-compliance. Copying and pasting another company's policies rather than undertaking a site-specific review is a call for enforcement officials to investigate — a call than can be and should be avoided.

---

**David J. Shaw** is a shareholder with Kirton McConkie in Salt Lake City, where devotes his practice to e-commerce and technology matters. He can be reached at 801-328-3600 or at dshaw@kmclaw.com.