

The Metropolitan Corporate Counsel®

www.metrocorpcounsel.com

February 2013

© 2013 The Metropolitan Corporate Counsel, Inc.

Volume 21, No. 2

FTC Updates To Online Privacy Acts, COPPA And VPPA

The Editor interviews Gina Reif Ilardi, Associate, Sheppard Mullin Richter & Hampton LLP.

Editor: Please start our discussion with an overview of the Children's Online Privacy Protection Act (COPPA) and the Video Privacy Protection Act (VPPA).

Ilardi: The Children's Online Privacy Protection Act ("COPPA") was enacted to place parents in control over what information is collected, used and disclosed from young children online. COPPA applies to operators of commercial websites and online services directed to children under the age of thirteen that collect, use, or disclose personal information from children, and to operators of general audience websites or online services with actual knowledge that they are collecting, using or disclosing personal information from children under thirteen. COPPA prohibits website operators from knowingly collecting information from children under the age of thirteen unless the operator obtains parental consent and allows parents to review their children's information and to restrict its further use.

In order to ensure compliance with COPPA, website operators must: (i) post a clear and comprehensive privacy policy on their website describing their information practices for children's personal information; (ii) provide direct notice to parents and obtain verifiable parental consent (with limited exceptions) before collecting personal information from children; (iii) give parents the choice of consenting to the operator's collection and internal use of a child's information, but prohibiting the operator from disclosing that information to third parties; (iv) provide parents access to their child's personal information to review and/or have the information deleted; (v) give parents the opportunity to prevent further use or

online collection of a child's personal information; and (vi) maintain the confidentiality, security and integrity of information they collect from children.

The Video Privacy Protection Act (the "VPPA") was passed in reaction to the disclosure of Supreme Court nominee Robert Bork's video rental records in a newspaper. The VPPA is not often invoked, but stands as one of the strongest protections of consumer privacy against a specific form of data collection. Generally, it prevents disclosure of personally identifiable rental records of "pre-recorded video cassette tapes or similar audio visual material." The VPPA has several important provisions, including: (i) a general ban on the disclosure of personally identifiable rental information unless the consumer consents specifically and in writing; (ii) prohibiting the disclosure of personally identifiable rental information to police officers unless there is a valid warrant or court order; (iii) exclusion of evidence acquired in violation of the VPPA; (iv) civil remedies, including possible punitive damages and attorneys' fees, not less than \$2,500; and (v) a requirement that video stores destroy rental records no longer than one year after an account is terminated. It's also worth noting that many states have enacted laws providing greater protections than the federal VPPA. Video rentals in Connecticut and Maryland, for example, are considered confidential and cannot be sold. California, Delaware, Iowa, Louisiana, New York and Rhode Island have also enacted video privacy laws. Michigan's video privacy law goes beyond the VPPA and protects records of book purchases, rentals and borrowing as well.



**Gina Reif
Ilardi**

Editor: The Federal Trade Commission (FTC) recently enacted updates to both Acts. What is the substance of these updates?

Ilardi: On December 19, 2012, The FTC announced the adoption of its long-awaited amendments to COPPA. The updates are primarily aimed at mobile privacy, but are intended to reflect the FTC's commitment to "helping to create a safer, more secure online experience for children" in the face of rapid technological change. The amended rule will be effective July 1, 2013. Some of the key changes to COPPA include:

(i) Modifying the definition of "personal information" to include "geolocation information sufficient to identify street name and name of a city or town" and photographs, videos or audio files "where such file contains a child's image or voice."

(ii) Revising the "persistent identifier" element in the definition of personal information to cover identifiers that "can be used to recognize a user over time and across different websites or online services," specifically including Internet Protocol ("IP") addresses.

(iii) Expanding and clarifying the accepted methods for obtaining verifiable parental consent to respond to evolving technology. For example, a signed parental consent form may now be returned to the website operator by "electronic scan" and consent may be provided to "trained personnel via video-conference."

(iv) Adding an exception to the requirement to provide notice and obtain verifiable parental consent where an operator "collects a persistent identifier and no other personal information and such identifier is used for the sole purpose of providing support for the internal operations of the website or online service."

(v) Imposing a new requirement that personal information collected from children be retained only "as long as is rea-

Please email the interviewee at gilardi@sheppardmullin.com with questions about this interview.

sonably necessary to fulfill the purpose for which the information was collected” and deleted “using reasonable measures to protect against unauthorized access to, or use of, the information in connection with its deletion.”

(vi) Prohibiting applications and websites directed at children from using third parties to collect children’s personal information through plug-ins unless parental notice is given and consent is obtained, and in some cases, such third parties will be responsible for complying with COPPA.

On January 10, 2013, President Obama signed into law amendments to the VPPA that facilitate social media sharing of video viewing preferences when users consent to disclosure of information via the Internet. The amendments provide that a consumer’s written consent can now be obtained through electronic means using the Internet, provided that the consent is in a “form separate and distinct from any form setting forth other legal or financial obligations of the consumer.” The amendments also permit the consumer to choose between giving consent to disclosure either: (1) in advance for a set period of time, up to two years or until consent is withdrawn, or (2) each time disclosure is sought (like under the old statute). Finally, the service provider must give the consumer “in a clear and conspicuous manner” the opportunity to withdraw consent either on a case-by-case basis or from ongoing disclosures, at the consumer’s election.

Editor: What is the business impact on companies like Netflix and Facebook of the VPPA update that eases restrictions on sharing a user’s online video rental/viewing history?

Iardi: The business impact of the VPPA revisions is significant. Netflix, which was a strong advocate for the amendments of the VPPA, is now planning to launch a Netflix Facebook App this year, an initiative that would have been next to impossible under the old VPPA. Prior to the recent amendment, the VPPA required “video tape service providers” to obtain the informed, written consent of consumers at the time disclosure of their personal information was sought. As such, providers like Netflix were largely unable to secure the type of ongoing customer consent necessary to provide certain social media features – such as Facebook integration – that are available to users outside

the United States. The changes to the VPPA make obtaining the requisite customer consent much easier, by allowing consumers to grant consent via electronic means on the Internet for up to two years. In turn, service providers must obtain the consent on a separate form (distinct from other forms used to disclose legal or financial obligations), and must provide customers the opportunity to withdraw consent on a case-by-case basis or to withdraw consent from ongoing disclosures. The ability to obtain advance consent from customers offers increased flexibility for “video tape service providers” and is expected to lead to tighter integration between such video providers and social networks, such as Facebook and Twitter.

Editor: Please discuss the COPPA update that expands the definition of “personal information.” Does this expanded definition apply only to COPPA, or might it be applied more generally?

Iardi: The expansion of the definition of “personal information” is arguably the most important change to the rule. The FTC made these changes in order to address various forms of new data that the FTC considers now personally identifiable. For example, under the revised rule, “personal information” now includes (i) screen or user names in cases where these identifiers function as “online contact information” as defined in the rule; (ii) photographs and video or audio files containing a child’s image or voice; and (iii) geolocation information. In addition, the FTC broadened the meaning of the term “persistent identifier” as it applies to personal information. Under the previous rule, a persistent identifier (e.g., a website cookie, IP address or a device serial number) must be linked to other information relating to a child or parent before it is classified as “personal information.” Under the revised rule, a persistent identifier standing alone is considered “personal information” in instances where it can be used to recognize a user over time and across different websites or online services, except where the identifier is used solely to support the internal operations of the website or online service. In addition, a mobile device’s unique identifier, or other identifier that can link a child’s activities across different websites or online services, falls within the “personal information” definition under the revised Rule. This new broadened definition of

“personal information” only applies to COPPA, but given the ever-changing landscape of privacy law in the U.S., it wouldn’t be surprising to see amendments to other laws and new legislation addressing similar issues in different contexts.

Editor: Are there any safe harbor protections available? If so, under what circumstances?

Iardi: An industry group may avoid compliance with COPPA if the group generates self-regulatory guidelines approved by the FTC. An industry group can request approval for such guidelines by providing the FTC with the proposed guidelines and an accompanying commentary showing compliance of the guidelines with COPPA. Such proposed guidelines must contain requirements that are substantially similar to COPPA, a mechanism for evaluation of the operators’ compliance with the guidelines, and incentives for compliance. Suggested mechanisms to determine compliance include periodic and random reviews of operators’ practices, periodic industry or independent reviews of practices of all subject operators, and comprehensive information practices reviews as a condition of membership in self-regulatory programs.

Editor: Going forward, what are the key components of effective online privacy policies?

Iardi: An effective online privacy policy should disclose all of the ways in which a website collects personally identifiable and non-personally identifiable information and how that information is used. For example, does the website use cookies to collect information about its users? Does the website work with third parties to collect information about its users or provide personal information to third parties? Does the website use Twitter or Facebook application programming interface (“API”) to link to users Facebook and/or Twitter accounts? If so, all of those practices should be disclosed in the privacy policy. The privacy policy should also inform users about how they can access and manage the data they have provided to the website and provide users with contact information for any questions or concerns they might have about the privacy policy and the use of their data. Finally, and most importantly, companies should comply with their privacy policy at all times and consistently review and update it in light of evolving law and policy.