THE
NATIONAL LAW REVIEW

Amendments in California's Online Privacy Law Addressing "Do Not Track" Disclosures May Put Website Operators at Risk

Friday, December 6, 2013

A recent amendment to California's existing online privacy legal framework aims to provide more transparency regarding how website operators use and share personally identifiable information ("PII") about an individual consumer's online activities over time and across different websites. California's online privacy law requires an operator of a commercial website or online service that collects PII to conspicuously post its privacy policy and identity what categories of PII are collected and with whom that information is shared. Most internet users are familiar with the concept of online data collection and online tracking, but what types of information websites are collecting about individual users and how websites are using that information is not always clear or readily apparent. The amendment to California's online privacy law aims to address this issue by requiring an operator to disclose how it responds to "do not track" signals or other browser-based mechanisms that purport to provide consumers with a choice regarding the collection of PII. Operators' failure to comply can result in civil liability and/or fines, but proper disclosures can avoid such liability.

Article By Michael B. GraySarah E. Smith Lee J. EulgenNeal, Gerber & Eisenberg LLP Alert

Consumer Protection
Communications, Media & Internet
Administrative & Regulatory
California

California Online Privacy Protection Act of 2003

In 2003, California enacted the Online Privacy Protection Act of 2003 ("CalOPPA"), which was the first state law in the United States to require owners of commercial websites or online services – including mobile app developers – to post a privacy policy. CalOPPA requires any person or company that operates a website or online service that is accessible to, and collects PII from, California consumers to conspicuously post a privacy policy. Under CalOPPA, an operator's privacy policy must specify the categories of PII that the operator collects and how it is used and shared with third parties.

Because the law applies to all residents of California and is potentially enforceable outside of the state's borders due to the transient nature of commercial websites, CalOPPA effectively compels all commercial sites, no matter where they are located, to update their policies to provide the proper disclosures. Failure to comply with CalOPPA may subject a website operator or a mobile app developer to civil liability for unfair business practices. While there is no private right of action, the California Attorney General can enforce the law, and penalties for a violation impose a maximum civil penalty of $2,500 per violation. Additionally, operators that violate CalOPPA may also be susceptible to actions by the Federal Trade Commission, which may bring enforcement actions against businesses whose posted privacy policy is deceptive, *i.e.,*where the business fails to comply with its posted privacy policy.

Privacy Concerns With "Do Not Track" Settings

While 2003's CalOPPA addressed the issue of what types of PII are collected and with whom PII is shared, it did not address how websites treat web browsers' "do not track" ("DNT") setting, which varies among websites. DNT settings purport to provide consumers with the ability to exercise control regarding PII collection over time and

across third-party websites. Most web browsers, including Mozilla's Firefox, Apple's Safari, and Google Chrome, allow users to select a DNT option that, in theory, blocks third party tracking across a network of websites. However, not every website honors other browser's DNT signals or blocks third party tracking. The inconsistencies in DNT practices may affect consumer's expectations regarding the collection and use of their online activities, particularly if they have opted out of such online tracking. The new 2013 amendment to CalOPPA aims to address this inconsistency.

The 2013 "Do Not Track" Law

California recently passed amendments to strengthen CalOPPA that require websites that collect PII to detail how they respond to DNT settings in web browsers, and operators must specify whether third parties can access any PII they collect. Although the amendments to CalOPPA do not require website operators to honor DNT signals or otherwise block third party tracking, the amendment (known as "AB 370") requires affected operators to update their privacy policy and include more disclosures regarding the website's tracking practices.

As noted above, AB 370 specifically applies to the use of PII to track users across time and over multiple websites. It requires that operators disclose whether third parties may collect PII about an individual consumer's online habits as he or she moves from one website to another. For example, a website operator may know that an individual customer is a 38-year-old male who lives on 555 Park Boulevard in San Diego, purchased a camera and booked a hotel online last week and has also visited numerous travel websites within the past two weeks. The collection of user's PII and online behavior can be a valuable tool in that it allows website operators to better identify and understand their customers, which may lead to more targeted (*i.e.* relevant) online advertising to those same customers as they move from one website to another. However, many internet users prefer not to be tracked online and utilize web browsers' DNT setting to prevent tracking.

The amendments to CalOPPA take effect on January 1, 2014, and affected operators have 30 days to comply after being notified of noncompliance to update their privacy policies. Failure to do so may subject operators and developers to fines of up to $2,500 per violation.

Practice Tips

Operators and developers of commercial websites, software and mobile apps that collect and transmit PII should review how their online service responds to web browsers "do not track" signal and whether they allow for the use of PII to track users across time and over multiple websites, and operators should timely update their privacy policies to disclose such tracking activities and should update their policies over time as their practices change.