SQUIRE SANDERS

# CALIFORNIA PASSES THE FIRST "DO-NOT-TRACK" LEGISLATION IN THE US

October 2013

## Introduction

On September 27, 2013, Governor Brown of California signed into law an amendment (Amendment) to California's Online Privacy Protection Act (CalOPPA) that represents the first attempt to implement "Do-Not-Track" legislation in the US, and that will require operators of websites and online services, who fall within the ambit of CalOPPA, to make changes to their consumer-facing privacy policies.

## CalOPPA

California remains the only state that requires all commercial Internet website or online services that collect personal information from state residents to post a privacy policy. Under CalOPPA, an operator of a commercial Internet website or online service that collects personally identifiable information through the Internet about consumers residing in California who use or visit its commercial website or online service is required to conspicuously post a privacy policy on its website or online service and to comply with that policy. Additionally, the privacy policy must specify the categories of personally identifiable information that the operator collects about individual consumers who use or visit its website or online service, as well as third-parties with whom the operator shares the information.

## Amendment Requirements

Under the Amendment, the privacy policy required by CalOPPA must now also disclose the following:

- whether other parties (e.g., third-party advertising networks and analytics providers) 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; and
- 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.

The Amendment does not provide a definition of "Do-Not-Track" or "consumer choice mechanisms." Generally, "Do-Not-Track" refers to technology that enables users, through an HTTP header, to opt out of online tracking by, among others, analytic services, advertising networks and social platforms. Notwithstanding the Federal Trade Commission's 2010 report calling for a standard Do-Not-Track system, to date efforts at standardization by the World Wide Web Consortium's Do-Not-Track Working Group have not been successful and there is not yet an established definition of "tracking".

## Compliance and Practical Recommendations

The Amendment imposes only a disclosure requirement. It does not require website operators to actually take any specific action with respect to the collection by third-parties of personally identifiable information about consumers' online activities (e.g., action preventing or limiting such collection), nor does it require operators to respond to Do-Not-Track signals in a certain manner. Operators only need to disclose whether third-parties may have access to personally identifiable information on operators' websites and whether, and if so how, operators respond to Do-Not-Track signals. If an operator does not respond to such signals, it will suffice merely to indicate this fact in the privacy policy; if an operator responds in some way to such signals, the privacy policy should disclose how the operator responds. The Amendment expressly allows operators to satisfy the Do-Not-Track disclosure requirement by information set forth in a separate online location accessible via a clear and conspicuous hyperlink in the operator's privacy policy.

Operators of websites and online services will be in violation of the new disclosure requirements only if they fail to address deficiencies within 30 days after being notified by the Attorney General of noncompliance. Nonetheless, at this early stage, given ongoing uncertainties regarding the very definition of "tracking," operators, in reviewing their practices and updating existing consumer-facing privacy policies to comply with the Amendment, should consider adopting a conservative approach that broadly interprets "Do-Not-Track" signals and "consumer choice mechanisms," and does not tie these to any particular format or technology. Additionally, operators should always bear in mind that their actual practices must be consistent with the information provided in their privacy policies in consequence of the new required disclosures. Any discrepancy between actual practice and information in a privacy policy creates the risk of action by the Federal Trade Commission.

## Contacts

**Ivan Rothman**
+1 415 954 0241
ivan.rothman@
squiresanders.com

**Philip Zender**
+1 415 393 9827
philip.zender@
squiresanders.com