SEYFARTH SHAW

International Data Privacy Client Alert

California Privacy Policy Law - Tracking Consumer Behavior Now Must be Disclosed

In 2003 the California legislature enacted §22575 of the business and professions code into law. It required commercial websites or online services that collect personally identifiable information (PII) about consumers residing in California to post a privacy policy. Under both California and federal law, this privacy policy must be adhered to by the operator of the website or online service. As of September 27, 2013 two new disclosure requirements have been added to §22575. As a result, all commercial entities that collect PII from consumers in California will need to re-evaluate their underlying technology and privacy policies for compliance.

Prior Requirements

Under the 2003 enactment, privacy policies needed to 1) identify categories of PII to be collected, 2) identify categories of the third parties with whom such PII would be shared, and 3) identify the processes for consumers to review and request changes to their PII in the event that the consumer felt that such information was inaccurate. For the most part, the privacy policy was not required to state the specific uses of the PII by either the website operator or any third parties to whom such PII was transferred.

This lack of transparency regarding the use of PII has led the California legislature to update §22575. With the passage of Assembly Bill 370, two new disclosures are now required of any privacy policy: 1) how a site responds to "Do Not Track" ("DNT") browser signals, and 2) if third parties can do behavioral tracking via the website.

New Disclosure #1: Response to "Do Not Track" Signals

Section 22575(b) now requires disclosure of how an operator responds to DNT signals. "Do not track" refers to a standards initiative by which browser settings can be used to send a signal to advertising networks, that are integrated into sites, indicating that the user of the browser does not wish to have their browsing habits tracked across websites over time.

All the major browser companies have incorporated DNT signal recognition into the latest releases of their browsers. However, there is no consistent deployment of this technology with regard to defaults or use cases. Section 22575(b)(5) also includes "other mechanisms" which can be used to provide consumers the ability to exercise choice regarding behavioral analysis of their browsing habits. Since most persistent technology embedded in a browser (e.g. cookies) can be used to observe browsing habits over time, careful evaluation of what technology a site uses, and how it is used, is necessary to determine if the new section's requirements are triggered.

Since the statute also applies to "online services," mobile app developers and any other business that provides a service accessible via a computer or smart phone are going to be required to provide notice as well.

As §22575 attempts to limit the mandatory disclosure to those operators who engage in collection for purposes of behavioral tracking, a careful review of current policy disclosures, and any technology imbedded into the site will need to occur–primarily because all websites and online services use technology which **may** be used to track users. Consequently, to ensure compliance with the new section, all privacy policies should include a statement indicating whether or not an operator actually allows the consumer to exercise a choice or not.

New Disclosure #2: Third-Party Behavioral Tracking

Along with the new DNT requirement, the privacy policy also must disclose whether or not third parties can collect PII for purposes of behavioral targeting when a consumer uses a website or online service. This is an inherently intrinsic activity for many websites and online services, especially those supported by advertising.

Because of the nature of third-party use, it will become increasingly difficult for an operator to provide notice of use of PII by a third party when the operator does not know how - or for what purposes - the third party is using the data. Even in instances where the operator *does* know the primary use of PII by the third party, such use may change over time. Since such disclosures and privacy policies are enforceable under state and federal deceptive trade practices acts, the new law now imposes an obligation on the operator to provide "guarantees" around how a third party may use data collected from the operator's website or through the operator's online service.

Given the variability of business and technology models underlying most website and online services, operators should engage competent counsel to help them navigate through a careful drafting process and to ensure adequate disclosures are included in their privacy policy under the new law. Further, operators will need to create and follow some level of process so they know with as much certainty as possible, the technology being deployed by third parties on their websites and/or online services.

By: *John P. Tomaszewski*

John P. Tomaszewski is a member of the Privacy & Data Security team, and is located in Seyfarth Shaw's San Francisco office. If you would like further information please contact your Seyfarth attorney or John Tomaszewski at *jtomaszewski@seyfarth.com*.