MEMORANDUM

TO: ESPC

FROM: D. Reed Freeman, Jr.

Julie O'Neill

Adam Fleisher

DATE: September 13, 2013 FILE: 68223-0000001

RE: Cal AB 370: Do Not Track comes to CalOPPA

I write to update you on a significant new state law development.

California's AB 370, if signed by Governor Jerry Brown, would be the first piece of legislation in the world addressing "do not track" ("DNT") directly to become law. It has passed both houses of the California Legislature and would likely take effect in January. The bill, which would amend California's existing Online Privacy Protection Act ("CalOPPA"),[1] requires website operators to explain how they respond to DNT 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 Web sites or online services, if the operator engages in that collection."[2]

Like California's data breach notification law, this would be a disclosure law, not a law creating new consumer rights or imposing substantive requirements on companies. That said, like the data breach notification law before it, its aim seems to be to pressure companies to make substantive changes (here, by responding to DNT signals; in the case of the breach notification law, by developing better data security practices in order to reduce the frequency of embarrassing disclosures).

Because CalOPPA applies to any website, online service or (according to the California Attorney General) mobile application that collects personally identifiable information from "consumers residing in California" (each, a "Site"), the law, if enacted, would have a *de facto* nationwide reach. As a result, while there have been rumblings about federal DNT legislation, California would set a new nationwide disclosure standard.

---

[1] Cal. Bus. & Prof. Code §§ 22575 *et seq.*

[2] *See* id. § 22575(5).

The big question, however, is what exactly Site operators would need to disclose. The challenge they would face is made particularly acute by the fact that the meaning of DNT is not clear, nor clearly defined, in the law itself or by industry, in spite of more than two years of negotiations at the World Wide Web Consortium ("W3C").

WHAT IS CalOPPA?

CalOPPA currently requires Site operators to post a privacy policy that does the following:[3]

- Identifies the categories of personally identifiable information collected;
- Provides a description of the process for an individual consumer who uses or visits a Site to review and request changes to his or her personally identifiable information that has been collected, if the Site offers such a process;
- Describes the process by which consumers will be notified of material changes to the privacy policy; and
- Identifies the effective date of the policy.

AB 370 AND "DO NOT TRACK"

Assuming the Governor signs AB 370—and it survives near certain legal challenges—Site operators will need to: (1) explain in their privacy policies how they respond to web browser DNT signals, and (2) disclose applicable third party data collection and use policies.

Before getting into the nuts-and-bolts of the new disclosure requirements, it might be helpful to step back to look at exactly what DNT is—or is intended to be. The idea behind a DNT mechanism is that it should provide consumers with an easy means to control the tracking of their online activities.[4] DNT is technically straightforward. When a DNT preference is enabled in a device browser or mobile app (including if it is enabled by default), the "DNT:1" header is transmitted to the requesting server along with other header information. DNT is intended to be an expression of the user's preferences regarding online tracking; however, the actual meaning of DNT—and what "honoring" DNT means—has been a considerable obstacle to its implementation. In other words, once the DNT header is received, what is the receiving server supposed to do?

For more than two years, a W3C working group has struggled with these issues. The collection and use of data by the Site the user is on (*i.e.*, the first party Site) may not be covered by the DNT opt-out. But what about third parties? The latest W3C working draft would bar third-party data collection, use, and sharing upon receipt of the DNT:1 header unless such collection, use, or sharing falls into an exception, such as fraud detection, marketing research, or analytics—and even those exceptions were vigorously contested.

---

[3] *See* id. §22575(b)(1)-(4).

[4] For more on the origins of the need to provide consumers with a DNT mechanism, see our client alert, *FTC Releases Draft Privacy Report Outlining Best Practices, Possible New Requirements Under Section 5 of the FTC Act, and Expressing Support for a "Do Not Track" List*, available at: http://www.mofo.com/files/Uploads/Images/101203-Do-not-track-list.pdf.

With the W3C process currently stalled and without a leader,[5] California has entered the fray, albeit without attempting to address these difficult and disputed questions.

WHAT DOES THE NEW "DO NOT TRACK" DISCLOSURE MEAN FOR SITE OPERATORS?

The amended CalOPPA would require Site operators to explain in their privacy policies how they respond to DNT 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 Web sites or online services, if the operator engages in that collection."[6]

The problem is what to say in order to comply with this requirement. Sites face the lack of a clear definition of what exactly DNT entails, and thus of how exactly to disclose their response to DNT signals. For now, it would be a mistake to represent that one "honors" DNT signals because that representation may be interpreted to mean more than the company's actions warrant. Assuming the bill takes effect, it would be best, for the time being, to comply with the facts: if your Site engages in activities triggering the required disclosure, do you do anything in response to the DNT:1 header? If not, say so. The law requires only a disclosure. If, on the other hand, you do something in response to receipt of a DNT:1 disclosure, say exactly what you do (*e.g.*, do you continue to collect data, but stop the creation of profiles for online behavioral advertising purposes?). This is a disclosure law, not a law establishing new consumer rights, and it can be breached by failure to disclose, or to disclose accurately, the required information.

The required disclosure may be made by link within an operator's privacy policy "to an online location containing a description, including the effects, of any program or protocol the operator follows that offers the consumer that [do not track or other] choice [mechanism]."[7] That is, there can be some central website or entity—perhaps even an industry self-regulatory website—that can provide an industry-wide response to the DNT question.

Finally, AB 370 addresses third party data sharing. It would require Site operators to disclose "whether other parties may collect personally identifiable information about an individual consumer's online activities over time and across different Web sites when a consumer uses the operator's Web site or service."[8] In other words, an operator must inform users about the data collection and use practices of *other* entities on its own Site, if those entities are also collecting data on different websites over time.

---

[5] Peter Swire resigned as the working group's head last week to focus on his new role on a privacy review board related to the National Security Agency data collection issues that arose over the summer.
[6] *See* Cal. Bus. & Prof. Code § 22575(5).
[7] *See* id. § 22575(7).
[8] *See* id. § 22575(6).

Since AB 370 simply expands the requirements of CalOPPA, the rest of the current CalOPPA regime will presumably apply. That means that Site operators will have violated the revised statute only if they fail to post a compliant privacy policy within 30 days of notice of noncompliance. Furthermore, while there is no private right of action, the California Attorney General can enforce the law. Any penalties for a violation would be under the California Unfair Competition Law, which imposes a maximum civil penalty of $2,500 per violation.[9]

While California has not by legislative fiat defined DNT or what honoring DNT means in terms of data collection and use, the prospect of new CalOPPA disclosure requirements certainly creates an additional incentive for the players in the online ecosystem to reach a consensus on what honoring DNT means. In the meantime, Site operators will have to be careful to avoid promising something that they cannot honor, if only because they cannot define it.

[9] *See* id. § 17206(a).