

Morrison & Foerster Client Alert

September 3, 2013

“Do Not Track” Comes to CalOPPA

By D. Reed Freeman, Jr., Julie O'Neill and Adam Fleisher

California's AB 370, if signed by Gov. Jerry Brown, would be the first piece of legislation in the world directly addressing “do not track” (“DNT”) 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 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.

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, despite more than two years of negotiations at the World Wide Web Consortium (“W3C”).

UNITED STATES

California

Tiffany Cheung	(415) 268-6848
Rebekah Kaufman	(415) 268-6148
Christine E. Lyon	(650) 813-5770
David F. McDowell	(213) 892-5383
James R. McGuire	(415) 268-7013
Daniel F. Muto	(858) 720-7959
Purvi G. Patel	(213) 892-5296
Andrew Serwin	(858) 720-5134
William L. Stern	(415) 268-7637
Nancy R. Thomas	(213) 892-5561
David M. Walsh	(213) 892-5262

New York

Cindy Abramson	(212) 336-4178
Melissa Crespo	(212) 336-4354
John F. Delaney	(212) 468-8040
Sherman W. Kahn	(212) 468-8023
Mark P. Ladner	(212) 468-8035
Peter McLaughlin	(212) 336-4290
Michael B. Miller	(212) 468-8009
Suhna N. Pierce	(212) 336-4150
Marian Waldmann Agarwal	(212) 336-4230
Miriam H. Wugmeister	(212) 506-7213

Washington, D.C.

Nicholas A. Datlowe	(202) 887-1590
L. Richard Fischer	(202) 887-1566
D. Reed Freeman, Jr.	(202) 887-6948
Julie O'Neill	(202) 887-8764
Obrea O. Poindexter	(202) 887-8741
Cynthia J. Rich	(202) 778-1652
Andrew M. Smith	(202) 887-1558
Nathan David Taylor	(202) 778-1644

EUROPE

Brussels

Joanna Łopatowska	32 2 340 7365
Karin Retzer	32 2 340 7364
Alja Poler De Zwart	32 2 340 7360

London

Ann Bevitt	44 20 7920 4041
Anthony Nagle	44 20 7920 4029
Caroline Stakim	44 20 7920 4055
David Varney	44 20 7920 4058

ASIA

Beijing

Gabriel Bloch	86 10 5909 3367
Jingxiao Fang	86 10 5909 3382
Paul D. McKenzie	86 10 5909 3366

Hong Kong

Gordon A. Milner	852 2585 0808
------------------	---------------

Tokyo

Daniel P. Levison	81 3 3214 6717
Gabriel E. Meister	81 3 3214 6748
Jay Ponazecki	81 3 3214 6562
Toshihiro So	81 3 3214 6568
Yukihiko Terazawa	81 3 3214 6585

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

² See *id.* § 22575(5).

Client Alert

WHAT IS CALOPPA?

CalOPPA currently requires Site operators to post a privacy policy that does the following³:

- 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. 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

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>.

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).

Client Alert

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.

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.

About Morrison & Foerster:

We are Morrison & Foerster — a global firm of exceptional credentials. Our clients include some of the largest financial institutions, investment banks, Fortune 100, technology and life science companies. We’ve been included on *The American Lawyer’s A-List* for 10 straight years, and *Fortune* named us one of the “100 Best Companies to Work For.” Our lawyers are committed to achieving innovative and business-minded results for our clients, while preserving the differences that make us stronger. This is MoFo. Visit us at www.mofo.com.

⁷ See id. § 22575(7).

⁸ See id. § 22575(6).

⁹ See id. § 17206(a).

Client Alert

Morrison & Foerster has a world-class privacy and data security practice that is cross-disciplinary and spans our global offices. With more than 60 lawyers actively counseling, litigating, and representing clients before regulators around the world on privacy and security of information issues, we have been recognized by *Chambers* and *Legal 500* as having one of the best domestic and global practices in this area.

For more information about our people and services and the resources we offer such as our treatise setting out the U.S. and international legal landscape related to workplace privacy and data security, "*Global Employee Privacy and Data Security Law*," or our free online Privacy Library, please visit: <http://www.mofo.com/privacy--data-security-services/> and "like" us on Facebook at <http://www.facebook.com/MoFoPrivacy>.

Because of the generality of this update, the information provided herein may not be applicable in all situations and should not be acted upon without specific legal advice based on particular situations. Prior results do not guarantee a similar outcome.