May 27, 2014

California AG Offers *Best Practices* for CalOPPA's Do Not Track Disclosures; Leaves Crucial *Compliance* Questions Unanswered

By Reed Freeman, Julie O'Neill, and Patrick Bernhardt

California Attorney General Kamala Harris released a long-awaited report entitled *Making Your Privacy Practices Public* (Report) on May 21, 2014. The Report recommends "best practices" for compliance with the California Online Privacy Protection Act (CalOPPA). It was originally intended to answer critical questions about exactly what website, online service, and mobile application operators (collectively, "site operators") must do to comply with CalOPPA's new do not track (DNT) disclosure obligations, which took effect on January 1, 2014. It does not accomplish that goal. Unfortunately, the Report leaves important questions unanswered *and* raises new questions.

The Report explains that "its recommendations . . . which in some places offer greater privacy protection than required by existing law, are not regulations, mandates or legal opinions."[1] It fails, however, to clarify what the law actually requires, and we expect that trade associations will continue to seek guidance on important compliance issues. In the meantime, site operators may wish to comply with at least some of the Report's recommendations to the extent possible because such "recommendations" tend to harden into regulatory "expectations" over time.

DISCLOSURE OF CROSS-SITE TRACKING AND RESPONSES TO DNT CHOICE MECHANISMS

In order to assess the Report's recommendations, it is important to first understand CalOPPA's DNT disclosure obligations. As amended by AB 370, the law requires a site operator to make disclosures with respect to:

[1] Report at 3.

UNITED STATES

California
Tiffany Cheung (415) 268-6848
Peter Day (650) 813-4231
Rebekah Kaufman (415) 268-6148
Christine E. Lyon (650) 813-5770
David F. McDowell (213) 892-5383
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
Michael B. Miller (212) 468-8009
Sotirios Petrovas (212) 336-4377
Suhna N. Pierce (212) 336-4150
Marian Waldmann Agarwal (212) 336-4230
Miriam H. Wugmeister (212) 506-7213

Washington, D.C.
Patrick Bernhardt (202) 887-8771
L. Richard Fischer (202) 887-1566
Adam J. Fleisher (202) 887-8781
D. Reed Freeman, Jr. (202) 887-6948
Libby J. Greismann (202) 778-1607
Julie O'Neill (202) 887-8764
Cynthia J. Rich (202) 778-1652
Andrew M. Smith (202) 887-1558
Nathan David Taylor (202) 778-1644

EUROPE

Berlin
Hanno Timner 49 30 72622-1346

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
Amy Collins 44 20 79204180
Susan McLean 44 20 79204045

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

Singapore
Daniel P. Levison 65 6922 2041

Tokyo
Toshihiro So 81 3 3214 6568
Yukihiro Terazawa 81 3 3214 6585

1. Its collection of personally identifiable information (PII)[2] about its users' activities over time and across third-party sites or online services, if it engages in such cross-site tracking; and

2. Any "other party's" tracking of the site operator's users over time and across third-party sites or services.

The law applies to cross-site tracking for any purpose, including, for example, analytics and advertising.

We discuss each of these obligations, as well as questions that the Report raises with respect to them, in turn as follows.

A. Disclosures relating to a site operator's own cross-site tracking.

The law requires that a site operator disclose *how* it responds to browser DNT signals or other tracking choice mechanisms, *if* it engages in cross-site tracking.[3] As the Report notes, "[t]he new provisions do not . . . depend on a standard for how an operator *should* respond to a DNT browser signal or to any mechanism that automatically communicates a consumer's choice not to be tracked."[4] The law requires only disclosure, not substantive practices, and it can be breached by a failure to disclose, or to disclose accurately, the required information.

What does this mean in practice and in light of the Report? And what questions does the Report raise?

- If a site operator engages in cross-site tracking, it must disclose how it responds to either browser DNT signals or another tracking choice mechanism.
    - *If a site operator engages in cross-site tracking and honors DNT signals*, it should explain *precisely* what it does in response to a DNT:1 header. Note that it may be a mistake to represent simply that a site operator "honors" DNT signals, as that representation could be interpreted to mean more than the operator's actions warrant.[5]
    - *If a site operator engages in cross-site tracking and honors some other means for users to express choice with respect to the tracking*, it should say so. The law permits a site operator to satisfy the DNT disclosure requirement by "providing a clear and conspicuous hyperlink in the 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 choice."[6] The Report makes it clear that a site operator may disclose *either* how it responds to a browser's DNT signal *or* link to another program or protocol that provides choice. The Report notes, however,

[2] The law applies only to companies that collect PII. In the online tracking context, where many companies do not collect names, addresses, or other "personal" information, this is an important limiting principle, and a potential defense, that the Report does not squarely address. The law itself defines PII broadly as information about a consumer that is collected online and maintained by the operator in accessible form, including name, address, email address, phone number, Social Security number, and, importantly: (a) any other identifier that permits the physical or online contacting of a specific individual; and (b) information concerning a user that the website or online service collects online from the user and maintains in personally identifiable form in combination with an identifier described in the definition. Cal. Bus. & Prof. Code § 22577(a)(6), (7). The California Attorney General seems to assume that this definition applies broadly to online tracking and thus triggers disclosure obligations. In fact, the Report specifically notes that the law's definition "can be understood to include information that is collected passively by the site or service, *such as a device identifier or geo-location data*." Report at 6 (emphasis added). For this reason, a site operator should be very careful to consider the types of information that it and its service providers collect, because, under the AG's interpretation, such collection may unwittingly subject it to the law's requirements, even if the site operator does not think of the data that it or its service provider collects as traditional "PII."

[3] Cal. Bus. & Prof. Code § 22575(b)(5).

[4] Report at 7 (emphasis in original).

[5] For example, there is not yet consensus among stakeholders across the spectrum of industry, academics, and advocates on whether honoring an opt-out means that the site operator ceases the online tracking or merely ceases using the information collected through such tracking.

[6] Cal. Bus. & Prof. Code § 22575(b)(7).

that "[d]escribing your response in your privacy policy statement is preferable to simply providing a link to a related 'program or protocol' . . . because it provides greater transparency to consumers."[7] It also recommends that site operators "[p]rovide the link *in addition to identifying the program with a brief, general description of what it does*."[8] While following these recommendations would promote transparency, both go beyond the law's requirement of providing a link.

The Report further recommends that a site operator consider whether "*the page to which you link* contain[s] a clear statement about the program's effects on the consumer . . . [and] what a consumer must do to exercise the choice offered by the program."[9]

This begs a couple of questions about linking to third-party choice programs:

1. **Must the link bring users directly to the program's opt-out page, or is a link to the program's website sufficient?** The Report does not make this clear and, again, may go beyond the law, which requires only a link to "an online location containing a description, including the effects, of any program or protocol the operator follows that offers the consumer that choice."

2. **The Report is silent as to which, if any, external choice programs are adequate.** In our judgment, industry self-regulatory programs such as those run by the Digital Advertising Alliance (DAA) and Network Advertising Initiative (NAI) should meet the law's requirements. But this is unsettled, and the AG has expressed concerns about whether either program meets the definition. We expect the NAI and DAA will seek further clarification on this point.

- *If a site operator engages in cross-site tracking but does not honor browser DNT signals or any other choice mechanism*, it should say that it does not honor browser DNT signals. With respect to such site operators, the Report recommends that "[i]f you do continue to collect personally identifiable information about consumers with a DNT signal as they move across other sites or services, *describe your uses of the information*."[10] While such a disclosure may be prudent—as a failure to make it could conceivably be deemed a material omission and thus deceptive under Federal Trade Commission law where such use may be unexpected by an ordinary user under the circumstances—the disclosure is not required by CalOPPA.

- **If a site operator does not engage in cross-site tracking, no disclosure obligation is triggered.**

B. Disclosures relating to another party's cross-site tracking.

CalOPPA requires that a site operator 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."[11] The law does not require the operator to make any disclosure regarding such "other party's" response to a DNT mechanism.

[7] Report at 11.

[8] *Id.* at 12 (emphasis added).

[9] Report at 12 (emphasis added).

[10] *Id.* at 11 (emphasis added).

[11] Cal. Bus. & Prof. Code § 22575(b)(6) (emphasis added).

What does this mean in practice and in light of the Report? And what questions does the Report raise?

- **Is a service provider an "other party"?** Because neither the law nor the Report clarify the meaning of the term "other party," it is not completely clear whether it includes a site operator's service provider or whether, on the other hand, a service provider stands in the site operator's shoes for purposes of the law. During a December 10, 2013 call with industry representatives, consumer advocates, and other interested parties, a representative of the AG's office suggested that a service provider is not the same as a site operator but instead should be treated as an "other party" for purposes of the law. This position is consistent with the law's definition of an "operator," which appears to exclude service providers.[12] In our judgment, it follows that a site operator *does not* have to disclose a DNT response or choice mechanism with respect to the cross-site tracking activities of its service providers, but it *does* have to disclose whether any service provider or other third party is engaged in the cross-site tracking of the site operator's users.[13]
- **The Report recommends that a site operator explain how a third party's practices may diverge from the site operator's DNT policy.**[14] This recommendation goes beyond the law's requirements. As discussed above, the law requires only that a site operator disclose *whether* third parties engage in cross-site tracking. It does not impose any requirement to address the third party's response to DNT signals or other choice mechanisms. The recommendation, however, raises the question of whether the AG believes there is a duty under the law for a site operator to vet the practices of third-party trackers on its site and to disclose whether such practices diverge from the site operator's own.

OPPORTUNITY TO CURE?

The Report acknowledges that CalOPPA includes a 30-day notice and cure period for noncompliance, but it does not squarely address whether that 30-day period applies to companies that have posted a privacy policy that fails to include required DNT disclosures but otherwise complies with the law. In a December 2013 call with interested stakeholders, a representative of the AG's office stated that the 30-day period *does not apply* in this situation, and this interpretation seems to be supported in the Report, which notes that "[t]he law provides an operator with a 30-day period *to post a policy after being notified of failure to do so*. *An operator subject to the law is in violation for failing to comply with the legal requirements for the policy* or with the provisions of its policy either knowingly and willfully or negligently and materially."[15] The AG's apparent interpretation is that the notice and cure provision applies only if there is *no policy whatsoever*, but that if there is any policy—even one that is almost completely compliant—then no notice and cure period is required. As a matter of public policy, this position makes no sense: the operator who did nothing should not be entitled to greater protection than the operator who tried hard and just missed the mark.

[12] *See id.* at § 22577(c). ("The term 'operator' means any person or entity that owns a Web site located on the Internet or an online service that collects and maintains personally identifiable information from a consumer residing in California who uses or visits the Web site or online service if the Web site or online service is operated for commercial purposes. It does not include any third party that operates, hosts, or manages, but does not own, a Web site or online service on the owner's behalf or by processing information on behalf of the owner.")

[13] As a practical matter, this distinction may be of no consequence: a site operator that uses a service provider for cross-site tracking (e.g., for analytics or behavioral advertising services) is typically contractually required by the service provider to both disclose the tracking and tell its users how they can opt out of it, such as through the DAA and/or NAI.

[14] Report at 12 (emphasis added).

[15] Report at 6.

ONLINE TRANSPARENCY "BEST PRACTICES"

Finally, the Report recommends other "best practices" aimed at ensuring that a site operator's privacy policy is transparent to its users. While many of these go beyond the law's requirements, it is worthwhile to consider them, as "best practices" tend over time to harden into regulatory expectations. They include the recommendations to:

- Prominently label the section of your policy regarding online tracking. For example: "California Do Not Track Disclosures."
- Disclose whether third parties collect PII from your users.
- Explain your uses of PII beyond what is necessary for fulfilling a customer transaction or for the basic functionality of the website or app.
- Describe what PII you collect from users, how you use it, and how long you retain it.
- Describe the choices a consumer has regarding the collection, use, and sharing of his or her PII.
- Use plain, straightforward language that avoids legal jargon, and use a format—such as a layered approach—that makes the policy readable. Use graphics or icons instead of text.

CONCLUSION

When it comes to compliance with the new CalOPPA DNT disclosure requirements, the Report raises more questions than it answers. It acknowledges that its recommendations are not necessarily legal requirements, but, in so doing, fails to clarify what the law itself requires. In light of this uncertainty, a site operator may wish to implement the Report's recommendations to the extent possible.

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.

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.