November 22, 2019

IS 'DO NOT TRACK' THE NEW 'DO NOT SELL'?

by Richard S. Eisert

It's been more than a month since the California Consumer Privacy Act (CCPA) draft regulations were released by the state attorney general's office, and rather than demystifying the CCPA, we are left with more puzzling details to parse.

Among those is: Do certain changes to user privacy settings now constitute full-blown CCPA opt-out requests?

New in the draft regulations is a requirement that businesses that collect a California consumer's personal information online must treat signals from "user-enabled privacy controls," indicating consumers don't want their personal information to be sold, as opt-out requests, otherwise known as "Do Not Sell" requests. These signals could come from a browser plug-in, privacy setting or any other user-enabled mechanism.

This is a completely new requirement absent from the statute itself. The California attorney general's office explained in its Initial Statement of Reasons that this new addition was "intended to support innovation for privacy services that facilitate the exercise of consumer rights in furtherance of the purposes of the CCPA." It said this was "necessary because, without it, businesses are likely to reject or ignore consumer tools."

What seems like a straightforward premise gives rise to the complex question of how exactly businesses are supposed to logistically translate these user-enabled privacy signals into the multistep procedures that accompany a CCPA opt-out request.

COMPLEX QUESTIONS

Would a default privacy signal count as a request not to "sell" the user's personal information? Equating passive default privacy settings to an opt-out request could render the CCPA's idea of an "opt-out" moot, and, instead, turn it into more of an "opt-in" right.

Even if default settings do not count as opt-outs, if a user intentionally sets certain privacy settings, how should those settings be interpreted and do they even align with what the CCPA intended the opt-out right to be?

For example, Do Not Track signals, which are web browser settings that request that websites not track user activity, could — assuming a website is even able to read those signals — be interpreted in many ways from site to site, as there is no uniform standard for what the signal means. Some current interpretations of the Do Not Track signal conflict with the effect of a CCPA Do Not Sell request.

Some sites interpret Do Not Track signals to mean no tracking (or sharing user personal information with others) at all. In contrast, Do Not Sell requests only restrict the "selling" of personal information as defined by the CCPA, which limits the sale or transfer of personal information but allows the publisher significant latitude in its own use of data that it collects directly from consumers.

The new CCPA regulations could turn the Do Not Track signal into a CCPA Do Not Sell request by default — and by doing so, create more questions about what the Do Not Track signal prohibits and what consumers are requesting when they enable such signals.

LOGISTICAL HURDLES

A Do Not Sell request also creates many logistical hurdles under CCPA, beyond what a Do Not Track or a simple disabling or enabling of cookies requires. Do Not Sell requests need to be implemented for a particular user or device across all of a business's platforms, both online and offline. Interpreting user privacy settings as an opt-out across all devices may not reflect a consumer's intent or even what their other devices or privacy controls indicate as a whole. The draft regulations appear to acknowledge this reality, but do not completely resolve the issue, by stating that the opt-out would apply broadly to the consumer only "if known" and otherwise only for the browser or device in question.

Even if the requirement applies only to the device sending the signal, what happens if there are contradictory signals or indications from the consumer? Some browsers allow users to separately control the Do Not Track and cookie settings. If the Do Not Track signal is enabled but the cookies settings allow all cookies, is the CCPA opt-out triggered or not triggered based on these settings?

And what about consumers who have their ad blockers turned off (or affirmatively turn them off to enter a website) but simultaneously have their Do Not Track signal enabled? Interestingly, the draft regulations may suggest a potential solution to this dilemma by stating that consumers can be offered a choice to opt out of sales of only certain categories of personal information. But it is far from clear how this choice mechanism would be reconciled with Do Not Track or other signals.

Beyond opt-outs, there is also a question of opt-ins. The CCPA requires that once consumers do opt out of sales of their information, businesses will have to wait 12 months before soliciting them to opt back into sales again. If a user's browser settings restrict the collection or sharing of their information, would the user, by undoing the settings without any solicitation, be opting back in, allowing businesses to resume selling their information? Conversely, would prompting a user to change their privacy settings always be considered an impermissible solicitation of a user to opt back in?

LITTLE CERTAINTY

These questions loom large for the ad tech ecosystem where consumer information is shared with multiple parties who will need to know whether that information is subject to opt-out requests or collected with CCPA-compliant notices before they can use it, often in real time. Organizations like the IAB are working to address this problem through the development of their own CCPA framework and technological tools that can send signals tracking CCPA opt-outs and notice for any consumer information being exchanged for programmatic advertising. Whether and how the IAB CCPA framework can be reconciled with the privacy settings requirement of the draft regulations creates even more ambiguity for the ad tech industry.

The one certainty in the wake of the draft regulations is that how privacy settings translate into opt-out rights will be a key issue in the public comments submitted before Dec. 6 for the attorney general's consideration. Perhaps in the final regulations, the attorney general may clarify that the "privacy settings" regulation only applies to CCPA-specific opt-out signals to be developed in the future, not all privacy signals in general.

But, on this point, the draft regulations are unclear, and we are left with more questions for the moment.

Follow Davis & Gilbert LLP (@dglaw) and AdExchanger (@adexchanger) on Twitter.

Richard S. Eisert is co-chair of the Advertising, Marketing & Promotions Practice Group and a partner in the Intellectual Property and Digital Media, Technology & Privacy Practice Groups of Davis & Gilbert. His clients include new media, technology and telecommunications companies, traditional publishing entities, advertisers, and advertising agencies. He may be reached at reisert@dglaw.com or 212.468.4863.