February 17, 2020

Choosing Your Chair for When the Music's Over: Seven Changes to the Proposed CCPA Regulations that Affect Your Privacy Operations

by John M. Brigagliano , Jon Neiditz

It's us again, back with more operationally-focused pointers on the California Consumer Privacy Act ("CCPA") now that the music has stopped once more and everybody is looking for a place to sit. On Friday February 7th, the California Attorney General released proposed amendments to the law's draft regulations. Although the updated draft regulations contain important omissions (e.g., they still do not provide statutorily mandated guidance regarding trade secrets), the amendments to the draft regulations provide some relief for businesses compared with the regulations' initial draft released last fall (they may even add a chair or two). The comment period for this round of changes to the regulations is open until February 25, 2020.

1. Personal Information Must be Linkable

Even information falling under an enumerated category of personal information in the CCPA is not necessarily personal information under then law. Information is not CCPA personal information if the information is not linked or *reasonably* linkable to a particular consumer or household. As an example, the regulations provide that IP address (since itself not directly identifying) is not personal information under the CCPA if the business collecting the IP address does not and cannot reasonably link the IP address to a particular consumer or household.

2. Just-in-Time Notice for Mobile Devices

The amended regulations provide a new requirement for providing the CCPA notice at collection in mobile environments. Importing FTC precedent, mobile apps that collect categories of personal information that consumers would not reasonably expect the apps to collect must provide a notice of the categories collected before the information's collection and a link to the organization's full notice at the point of collection.

3. Employee Notice

GDPR compliant (and likely other) organizations have a privacy notice for employees. Under the amended regulations, organizations can provide a link to or paper copy of that notice to satisfy the CCPA's requirement of an employee-facing notice at collection.

4. Extended Period for Rights Request Acknowledgement

The initial draft of the regulations required businesses to acknowledge receipt of CCPA rights requests within 10 days upon receiving such requests. Amendments to the regulations extend that period by providing 10 *business*

days to acknowledge such requests. That extension is only for acknowledgement; the time that businesses may take before providing a full response to rights requests remains 45 days unless extended.

5. Biometrics Excluded from Access Requests

In keeping with the prohibition on disclosing notice-triggering information under the breach law in response to access requests, that prohibition has been expanded to include some biometric information. Yet that prohibition does not apply to all information defined as biometric under the CCPA,which inexplicably includes in that definition information such as photographs and audio recordings from which biometrics could be captured. Instead, it is limited – as is the breach law – to "unique biometric data generated from measurements or technical analysis of human characteristics." Note that the breach law – unlike the draft CCPA regulation – goes on to explain what is and is not notice-triggering: "Unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual. Unique biometric data does not include a physical or digital photograph, unless used or stored for facial recognition purposes." Lawyers will be delighted and consumers sometimes confused by the three divergent definitions.

6. Expanded Information Uses for Service Providers

The initial draft of the regulations narrowly restricted service providers' uses of personal information. The amendments to the draft regulations respond to our entreaties by authorizing services providers to use personal information collected on their customers' behalf for their own critical purposes such as product improvement and analytics: "For internal use by the service provider to build or improve the quality of its services, provided that the use does not include building or modifying household or consumer profiles, or cleaning or augmenting data acquired from another source."

7. Device-Based Authentication

Businesses may honor deletion requests even with respect to information not maintained with any direct identifiers, such as name or email. Businesses may adjust verification methods for such circumstances. Therefore, for example, businesses that offer mobile apps for which an account is not required may use device-based authentication to verify a consumer pursuant to a deletion request. However, we note that businesses may also find that they have valid bases for not honoring such requests at all given the discussion of personal information's scope provided above and the CCPA's own limitation that business need not relink or reidentify information in order to comply with the law.

We'll be back in touch whenever the music pauses, for example when the regs are finalized, if and when the legislature does cleanups, and of course when the next ballot initiative is passed in California later this year, as we will when there are important developments in other states such as Washington. Like you, we will keep our eye on the eventual configuration of chairs when the music is finally over; we are well aware that's what you want to build and train on. And in that regard and speaking of Washington, the message of the excellent chart attached to this post drawn from the excellent broader comparison done by Stacey Gray, Pollyanna Sanderson, and Katelyn Ringrose of the Future of Privacy Forum may be that when the music's over, what is left will be

GDPR convergence except around lawful basis (which came not from GDPR, but from prior EU law). That may at least be the bet of many pro-privacy platforms that have interpreted their way out of “Do Not Sell My Personal Information” buttons. And this is no surprise, when the EU is letting it be known that it may exercise its powerful leverage by deeming the protections of individual U.S. states “adequate.” And if the laboratories of the states keep coughing up inconsistent products, there is always the possibility of dormant commerce clause cases pulling down the outliers. So we may see at least one version of the endgame, but we have a long, long way still to go….