May 5, 2022

Remarks of Chris Pedigo, SVP, Government Affairs, Digital Content Next

RE: Consumer Right to Opt Out

Good afternoon, my name is Chris Pedigo. I am the SVP for Government Affairs for Digital Content Next. DCN is the only trade association that exclusively represents publishers and focuses on the digital futures for thousands of trusted news and entertainment brands.

I'd like to first discuss how business practices are altered when a consumer exercises her choice to opt-out and then second how she technically makes this choice.

First, when a consumer opts out, the website or publisher cannot sell the consumer's data to a third party and should pass along this signal to any company which may have code on the app or website. Going forward, the consumer's data can only be collected and used by the publisher and its service providers, which are contractually obligated to use data only on behalf of the publisher to deliver the requested service and not for any secondary purpose. For instance, a news publisher and its service providers may use a consumer's data to remember a trusting subscriber's information or conduct analytics on the usage of the site or app. These types of uses are clearly in line with consumer expectations and facilitate the trusted, direct relationship between the consumer and the publisher. We were pleased the law does not limit this direct use by the publisher as it would harm its business interests.

With this dynamic in mind, Section 1795.135 (f) of the CPRA stipulates any third-party company which receives the opt out signal must immediately limit their use of that consumer's data to that of a service provider. We are very supportive of this provision for several reasons. It puts the onus for compliance on the company collecting data. It would be impossible for publishers to audit the data practices of all the third-party companies in the ecosystem. Another reason is that this section clearly lays out what companies can and cannot do with consumer data. Thus, it avoids the need for publishers to re-negotiate hundreds or thousands of contracts. These contract negotiations can be lengthy and expensive which takes resources away from the core business of creating news and entertainment. More importantly, as you can imagine, a few large tech companies could and have previously used their market dominance to negotiate

special terms in an effort to avoid the impact of privacy law. In short, we believe this section of the CPRA recognizes the complex and dynamic nature of the digital ecosystem and urge you to rebuff any attempts to undermine it.

Secondly, I would like to discuss the two methods by which consumers can opt out. One is to click on the Do Not Sell button on a website. The other is to use a global privacy control, which persistently sends an opt out signal to every website, app or third-party company that could potentially collect that consumer's data. The CCPA allows for authorized agents to send these kinds of opt out signals and the CPRA further clarifies this functionality. We believe global privacy controls are important because they give consumers an easy way to opt out of web wide tracking so they don't have to click on the Do Not Sell button on every website or app they visit. We've seen nearly 80% of Apple users make this choice to not be tracked. By aligning with users expectations, industry may grow consumer trust. And publishers have an opportunity to enhance their advertising offerings as they can target advertising based on direct subscriber relationship data, contextually and through other forms of privacy-friendly advertising. In enhancing consumer trust and the value of direct, trusted relationships, this law provides opportunity for publishers to capture some of the ad revenue growth as small businesses and large seek out new customers.

We are concerned, however, that some will attempt to undermine the effectiveness of global privacy controls in several ways. Some have suggested that the consumer should be required to take specific action to confirm or authenticate the signal. We believe this runs counter to the CPRA and the purpose of global privacy controls which are meant to reduce friction and rapidly align with consumer expectations without requiring additional data or effort. We believe the CPRA allows these signals to be turned on by default especially to the extent that the service markets itself as a privacy-enhancing tool. That said, we are concerned that browser or device companies, particularly those with market power, may seek to promote their own preference signals to unfairly favor their own business.

As you prepare draft regulations for the CPRA, I urge you do two things: One, ensure that global privacy controls are easy for consumers to use. Two, I urge you to reaffirm the text of the CPRA which stipulates that a third party must revert to the role of a service provider when a publisher or user agent communicates the consumer's opt out signal. I appreciate the opportunity to speak today and look forward to working with you in the future.