



April 17, 2019

The Honorable Jacqui Irwin
California State Capitol, Room 5119
Sacramento, CA 94249-0024

**Re: AB 873 – as introduced
OPPOSE**

Dear Assemblymember Irwin:

The undersigned coalition of organizations write to express our opposition to AB 873. This bill modifies the California Consumer Privacy Act by changing the definition of “personal information” and “deidentified.” Unfortunately, these changes would undermine necessary privacy protections under the CCPA. Respectfully, we must oppose the bill as written.

AB 873 makes three revisions to the definition of personal information in the CCPA. First, it removes “household” from the definition of personal information, threatening to undermine protections for information associated with a household (e.g., by an Internet Service Provider or a connected device). Second, it removes critical language that ensures that privacy protections for personal information take into account the modern realities of how personal information is stored and used. And third, it eliminates necessary safeguards in the definition of “deidentified” that require companies to take practical steps to ensure that information, once deidentified, stays that way.

The definition of personal information is the foundation on which privacy laws are built. Californians have demonstrated that they want a privacy law with a strong foundation that extends not just to information about them, but also about their households and devices as well. A poll of likely California voters, conducted last month by David Binder Research, showed that Californians overwhelmingly support a definition of personal information that encompasses all information about them.¹ Over 90% of voters, spanning across age, gender, party, and region of California, said it was important to be able to control their personal information in each of the following areas:

- Information related to or collected about a household – such as where you live, who you live with, or from a device in your home, such as Alexa, a baby monitor, or a household appliance like a “smart” TV or refrigerator.

¹ Will California lawmakers vote to protect Californians’ privacy or tech industry profits? ACLU of Northern California, March 27, 2019 (available at <https://www.aclunc.org/blog/will-california-lawmakers-vote-protect-californians-privacy-or-tech-industry-profits>).

- Information collected about your computer, phone or other device that allows companies to track you - over time.
- Location information – information about where you go including the history of where you’ve been.
- Inferences, meaning determining who you are, such as what you like or your race, gender, sexuality, and political and religious views, based on other personal information collected and shared.

Privacy laws must take into account the modern reality that anonymization techniques do not adequately protect information.² For example, “anonymized” search queries released by AOL were nonetheless associated with particular individuals.³ And Twitter users were unmasked by leveraging the structure of social relationships.⁴ Machine learning techniques can significantly reduce the difficulty of re-identifying personal information over time. Signaling the maturity of these re-identification techniques, data brokers are even offering what is effectively re-identification as a service, promising the ability to “reach customers, not cookies”.⁵ As written, AB 873 threatens to eliminate protections for information that has immense potential to violate people’s privacy. The CCPA’s definition of personal information should be maintained.

Finally, AB 873’s elimination of three critical safeguards in the definition of “deidentified” will undermine internal processes that protect information from re-identification. The CCPA requires that deidentified information must be accompanied by technical and business safeguards to protect information against re-identification. Civil Code § 1798.140(h). By removing these restrictions, AB 873 puts personal information at risk.

For these reasons, we must respectfully oppose A.B. 873 as written.

Sincerely,

Sean McLaughlin, Executive Director, Access Humboldt
 Kevin Baker, Legislative Director, ACLU of California
 Katharina Kopp, Ph.D. Deputy Director, Director of Policy, Center for Digital Democracy
 Ariel Fox Johnson, Senior Counsel for Policy and Privacy, Common Sense Kids Action
 Susan Grant, Director of Consumer Protection and Privacy, Consumer Federation of America
 Matthew Erickson, Executive Director, Digital Privacy Alliance
 Lee Tien, Senior Staff Attorney and the Adams Chair for Internet Rights, Electronic Frontier Foundation
 Tracy Rosenberg, Executive Director, Media Alliance
 Lou Katz, Member, Oakland Privacy
 Emory Roane, Policy Counsel, Privacy Rights Clearinghouse

Cc: Members and Committee Staff, Assembly Privacy and Consumer Protection Committee

² Nate Anderson, *Anonymized” data really isn’t—and here’s why not*, Ars Technica, September 8, 2009 (available at <https://arstechnica.com/tech-policy/2009/09/your-secrets-live-online-in-databases-of-ruin/>); see also Ohm, Paul, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, August 13, 2009. UCLA Law Review, Vol. 57, p. 1701, 2010; U of Colorado Law Legal Studies Research Paper No. 9-12 (available at SSRN: <https://ssrn.com/abstract=1450006>).

³ Eric Bangeman, *AOL subscribers sue over data leak*, Ars Technica, September 26, 2006 (available at <https://arstechnica.com/information-technology/2006/09/7835/>).

⁴ Nate Anderson, *Pulling back the curtain on “anonymous” Twitterers*, Ars Technica, March 31, 2009 (available at <https://arstechnica.com/tech-policy/2009/03/pulling-back-the-curtain-on-anonymous-twitterers/>)

⁵ *Reach Customers, Not Just Cookies*, LiveRamp Blog, September 10, 2015 (available at <https://liveramp.com/blog/reach-customers-not-just-cookies/>) (“Cookies are like an anonymous ID that cannot identify you as a person.”).