Testimony of

Ari Ezra Waldman, JD, PhD
University of California, Irvine School of Law

at the California State Assembly

Privacy and Consumer Protection
Informational Hearing

Tuesday, March 3, 2026
1:30 p.m., State Capitol, Room 437

Chairperson Bauer-Kahan, Vice Chair Macedo, Members of the Committee:

Today's information hearing is a crucial step toward building privacy law in true California fashion—namely, in ways that recognize, account for, and address the fact that some people, particularly those most marginalized in society, may have both a special need for privacy protection and are more likely to face disproportionate harm from surveillance.

My name is Ari Waldman and I am a professor of law at the University of California, Irvine School of Law. Much of my research is at the intersection of information technology, privacy, and queer civil rights, so thank you for inviting me here today to discuss these matters with you.

Thank you also for including in this hearing people like Mr. Black, whose direct experience of oversurveillance in service of someone else's profit in an oligarchic, informational capitalistic economy hammers home both the need for stronger privacy protections for our workers and the point that I want to make today: That the burdens of surveillance are not shared equally.

Those of us who study privacy all know a few very famous stories about how tech companies' voracious and endless appetite for engagement and advertising dollars, topics Professor Mulligan deftly discussed in her testimony, have undermined the privacy of the most vulnerable among us. First, there is the Target example. Long before the company folded its equity initiatives, it decided it wanted more of the market for baby products. So, company executives tasked their statisticians to hoover up data from its loyalty program among other places to try to find customers, and this is crucial, who are *about to be* pregnant.

The market for baby products is worth hundreds of billions of dollars, so, they figured, let's target—no pun intended—these customers before they start buying diapers and everything else new moms need somewhere else. You may say there isn't anything wrong with that, especially if these new moms are going to be given the chance to buy things on sale. But Target

used its data to essentially out a young woman as pregnant before she had the chance to tell anyone else in her family.

Second, there are the innumerable stories of Facebook outing its users as queer to their friends and families and anyone else in their network. As much as Meta's executives protest in public that they fixed this problem, the number of calls I get each year about this suggest that they haven't fixed much of anything. Facebook still likes to get users to engage by showing them how their friends have engaged. I wrote part of my doctoral dissertation on this point: Doing so manufactures a kind of social trust that triggers a cascade of engagement from others. If I know my friend did something or likes something, I'm more likely to do it or like it too. Anyway, Facebook routinely does this for affinity groups or products or businesses or many other things that indicate queerness, essentially outing many queer adolescents to the people who follow them.

Finally, there are darker examples of data-driven harms. Online harassment, particularly of women, is facilitated by a business model that prioritizes maximal data collection from maximal engagement. Data-driven algorithms feed users dangerous messages that push some people over the edge to severe depression and suicide. Of course this can happen to anyone, and it does. But queer kids, adolescent girls, marginalized boys, those living with disabilities, and many more are targeted more often.

Then there are stories we hear less about in the media, maybe because they happen so often that some people don't think they're news. Or because they don't fit the narrative a newspaper owned by Amazon's oligarch wants us to hear.

These are the stories about Joan (a pseudonym), a nineteen-year-old whose data was used by a dating website to target her with men who abused her.

There's Matthew, who was told by a dating app that there was nothing the company could do to stop someone from impersonating him and sending strangers to his home and place of business looking for sex. In several of those incidents, the impersonator assured the person they were talking to

that they shouldn't stop even if they—meaning Matthew—objected or protested or said no because they wanted to explore fantasies about sexual assault.

And there's Stephanie, who was murdered after being stalked by someone who got all the information he needed about her from a data broker.

And Mary, whose geolocation history was sent by Google to a state attorney general investigating her and her mother for going out of state to get an abortion.

Let's not forget this point: The data collected by private companies for capitalistic surveillance does not simply remain on the servers of those private companies. They share it with other companies.

And they also share it with the government. Allowing data-extractive behavior in the for-profit world gives hostile governments access to the data they need to punish people they don't like. This is what's happening to transgender people and their families in Texas and elsewhere. This is what's happening to some women seeking to exercise what rights they still have when they travel to pro-choice states to terminate their unwanted or dangerous pregnancies.

Just today, Joseph Cox at 404 Media reported that ICE and CBP used location data sourced from online advertisers to track phone locations of people they wanted to arrest. The ease with which the government can access privately-collected data and the eagerness so many oligarchs have shown to partner with this particular regime in Washington demonstrates that data collection by OpenAI or Meta can sometimes be little different than data collection by the Trump Administration.

The harms of this kind of data extraction may seem obvious, but allow me to highlight a few of them nonetheless. Data extraction driven by a pathological demand for engagement strips us of our autonomy. It treats us as merely means to someone else's end. It reduces us to numbers and metrics that see humans as merely fitting into categories like Romance

Novel Reading Urbanites or Christian Serial Daters or Susceptible to Splurge Purchases, all of which are real categories. These harms metastasize for the most marginalized among us, who are already told by society that they are less than or less deserving of protection. We see it everyday: the deaths by suicide, the harassment, the microtargeting, the misinformation, and other real social harms.

Some people, often those more technically inclined or those who trust technology to solve social problems for us, may tell you that the answer to the harms of data collection is actually to collect *more* data. To stop discrimination and harm, companies need more information about who we are and what is happening to us. In the AI context, computer scientists call this "fairness through awareness". The best way to stop disparate impact from AI systems is to let the AI take diversity into account.

Don't be fooled by this argument. It is a smokescreen to continue rampant, unregulated data collection on the backs of those who, sometimes, don't want the information collected in the first place. Why would those most susceptible to the harms of surveillance want private or public entities to surveil them more to make their products more accurate at surveillance? It just doesn't make sense.

Instead, California can take a different approach. We need an aggressive government regulator that is going to do more than require companies to draft up impact assessments and then file those assessments in some cabinet, digital or otherwise. I have written about the failure of this approach at length.

Instead, we need ongoing monitoring of corporate adherence to the civil right of privacy, where data-extractive products are limited in what they can collect, where personal data is not used to turn users into depressed, isolated, and suicidal addicts. We need to make it harder for government to gain access to privately collected data. We need to hold companies accountable when their products have disparate impacts on minoritized populations.

As my time comes to its end, I look forward to discussing even more specific steps in the q&a California can take to be a leader at protecting the privacy of its most marginalized citizens.

Thank you for your time.