

January 14, 2020

Attorney General Xavier Becerra
Office of the Attorney General
1300 I Street
Sacramento, CA 95814

Re: Norwegian Consumer Council's Report Demonstrates How the Adtech Industry Fails to Respect Consumers Rights and Preferences

Dear Attorney General Xavier Becerra:

We, the undersigned organizations, write to draw your attention to a report by the Norwegian Consumer Council (NCC) released today that examines apps and the advertising ecosystem that underlies them. The report, Out of Control: How Consumers Are Exploited by the Online Advertising Industry, examines 10 popular apps in the Google Play Store in several categories, including dating (Grindr, Happn, OkCupid, and Tinder); reproductive health (Clue and MyDays); makeup (Perfect365); religion (Qibla Finder); children (My Talking Tom 2); and a keyboard app (Wave Keyboard). Although the research for this work was completed in the EU, all of these apps are available to users in the US and many of the companies involved are headquartered in the US. The report shows how the online marketing and adtech industry operates to undermine consumers' privacy preferences and rights under the General Data Protection Regulation (GDPR). The report concludes that the comprehensive tracking and profiling of consumers that is at the heart of the current adtech ecosystem are, by their very nature, exploitative practices which do not respect the GDPR. In addition, many of the practices detailed within this report likely constitute unfair and deceptive practices that fall under your jurisdiction to investigate under your UDAAP authority and under the California Consumer Privacy Act.

We request that you review the report and investigate whether the practices detailed within the report constitute unfair or deceptive practices and whether they violate the privacy laws of your state.

Although there are ways consumers can control the number of trackers on computers through browser settings and extensions, the same cannot be said for smartphones. Indeed, as the report notes, "ad blockers and tracker blockers are often banned from the Google Play Store." While consumers use their smartphones throughout the day, the devices are recording information about sensitive topics such as their geolocation, health, behavior, interests, religion, and sexuality.

The report reveals how the hidden advertising structure of these apps receive and exploit consumers' personal data. Specifically, the report details the following issues:

- Personal consumer data is systematically collected, shared, and used by multiple businesses. Consumers also have no knowledge or control over such data sharing and use.
- In addition to being used to display targeted advertising, the comprehensive profiling and categorization of consumers can trigger different kinds of harm, both for the individual consumer and for society as a whole. This includes different forms of discrimination and exclusion, widespread fraud, manipulation, and the chilling effects that widespread commercial surveillance may have both on individuals and more generally on consumer trust in the digital economy.
- Consumers cannot avoid being tracked by these apps and their advertising partners because they are not provided with the necessary information to make informed choices when launching the apps for the first time.
- Consumers are unable to make an informed choice because the extent of tracking, data sharing, and the overall complexity of the adtech ecosystem is hidden and incomprehensible to average consumers. Thus, consumers are unable to make real choices about how their personal data is collected, shared, and used by myriad players in the adtech industry.
- Even if a consumer had a comprehensive knowledge of how adtech works, there would still be very limited methods to stop or control this data sharing and use. The number of actors and the complexity of the business arrangements between them in the adtech ecosystem, even if one considers only 10 apps, is staggering. For some apps, a consumer would be required to read through the privacy policies of over a hundred adtech partners in order to fully inform themselves of the extent to which their data will be shared and used. It is unreasonable to expect consumers to read over a hundred policies in order to decide whether or not to trust their sensitive data to an app and its business partners.
- Consequently, consumers have no meaningful way to inform themselves about the sharing practices of the many actors involved in sharing their data for any one app; and furthermore, they have no meaningful ways to restrict or otherwise protect their data.

This surveillance-business model increasingly has implications beyond our digital lives. The data abuses detailed in the NCC's research also contribute to the erosion of trust in the digital economy, could negatively impact our democratic processes, and may have discriminatory impacts. In addition, the report's findings demonstrate how these pervasive sharing agreements between apps and adtech companies undermine consumer choice and control over their personal data. The data abuses detailed in the NCC's research also contribute to the erosion of trust in the digital economy and has the ability to negatively impact our democratic processes.

On the basis of these findings, the NCC is filing a series of complaints before the Norwegian Data Protection Authority against various adtech companies and the dating app Grindr. We likewise urge you to investigate the issues detailed in the report because the practices detailed in the report may constitute unfair and deceptive practices. The practices detailed in the report may well be in

violation of the privacy laws in effect in your state, especially under the California Consumer Privacy Act. Finally, this report makes it clear that adequate enforcement of the few privacy laws we have is essential to protecting consumer privacy and choice.

Thank you for your attention to this matter.

Sincerely,
ACLU of California
Campaign for a Commercial-Free Childhood
Center for Digital Democracy
Consumer Action
Consumer Federation of America
Consumer Reports
Electronic Privacy Information Center
Public Citizen
US Public Interest Research Group