January 14, 2020

United States Senate
Washington, DC 20510

United States House of Representatives
Washington DC, 20515

***Re:	Adtech Industry Fails to Respect Consumers Rights and Preference, demonstrating the urgent need for a comprehensive privacy law and strong enforcement in the United States***

Dear Senators and Representatives:

We, the undersigned organizations, write to draw your attention to a groundbreaking report with far-reaching implication for American consumers, the US tech industry, and US-EU trade relations. At a time of growing support in the United State for stronger privacy law, a Norwegian consumer organization has uncovered widespread problems with several popular apps. The report also makes clear that several US firms may be in violation of the General Data Protection Regulation (GDPR), the European privacy law. If the United States fails to respond to the problems detailed in the report Out of Control: How Consumers Are Exploited by the Online Advertising Industry, released today by the Norwegian Consumer Council (NCC), the risks to consumers and trans-Atlantic trade will increase.

The report examines 10 apps in the Google Play Store and the underlying advertising apps ecosystem. The apps examined are from different 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 and popular in the US and many of the companies involved are headquartered in the US.

The report clearly demonstrates that the comprehensive tracking and profiling of consumers is at the heart of the current adtech ecosystem. We request that you review the report and commit to passing a strong, comprehensive federal privacy law that provides sufficient methods of and resources for effective enforcement.

The groundbreaking research reveals how apps enable commercial third parties to collect, use, and share sensitive consumer data. All of this sharing is hidden from the end user and involves parties that the consumer neither knows about nor would be familiar with. Unlike the apps they download, consumers do not have a first-party relationship with the variety of companies that will receive highly sensitive data about them. Although there are ways consumers can control some tracking on computers through browser settings and extensions, the same cannot be said for smartphones and tablets. 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, religion, interests, and sexuality.

While the report focuses on how these apps and their business partners in the adtech industry appear to be failing to comply with the requirements of the EU's GDPR, these practices also may constitute unfair and deceptive practices in the US. To that end, we are also sending letters to the Federal Trade Commission and selected state Attorneys General in order to bring their attention to the report's findings and request that they investigate these issues further. More generally, however, this report demonstrates the need for a strong, comprehensive baseline data privacy legislation and strong enforcement in the US at the federal level. Such a law also requires a strong data protection authority to enforce the law once it is passed. And any such authority will also require sufficient funding to ensure effective enforcement and compliance with the law's requirements.

Although the EU's GDPR went into force in May 2018, the report notes that "regulators are still struggling with receiving adequate funding" for enforcement activities. The report goes further, stating: "Consequently, enforcement seems to be lacking even when there is ample evidence of breaches of data protection legislation." This report not only makes it clear that we require a similar law in the US to protect consumer privacy and choice, but also that we must prioritize resourcing for enforcing any such law.

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.

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 request that you examine this report and commit to passing a comprehensive federal privacy law that not only protects the privacy and preferences of consumers, but also provides strong enforcement measures and sufficient funding to implement them. Further, we urge you to allow for consumers to bring private rights of action under any federal privacy law to ensure that consumers are able to pursue their own rights to redress in our courts.

Finally, it is worth reiterating that the report indicates U.S. companies are engaging in these practices even under GDPR. Therefore, we urge Congress to look to nonprofit organizations focused on protecting consumer interests and promoting consumer privacy, dignity, and choice when drafting any federal privacy law, rather than working closely with an industry that may be violating EU privacy laws.

Thank you for your attention to this matter.

Sincerely,
ACLU
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