The New York Times https://www.nytimes.com/2020/01/13/technology/grindr-apps-dating-data-tracking.html

# *Grindr and OkCupid Spread Personal Details, Study Says*

Norwegian research raises questions about whether certain ways of sharing of information violate data privacy laws in Europe and the United States.

Published Jan. 13, 2020 Updated Oct. 14, 2021

**By Natasha Singer and Aaron Krolik**

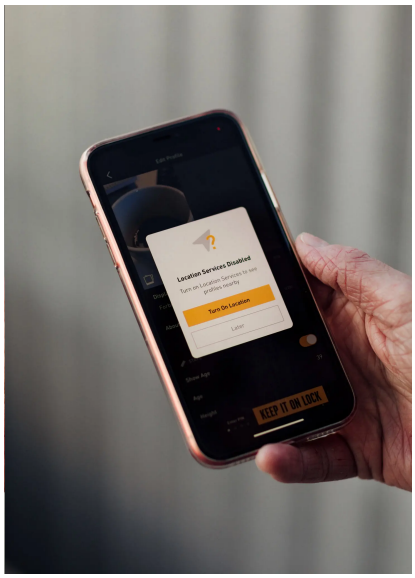
Popular dating services like Grindr, OkCupid and Tinder are spreading user information like dating choices and precise location to advertising and marketing companies in ways that may violate privacy laws, according to a new report that examined some of the world's most downloaded Android apps.

Grindr, the world's most popular gay dating app, transmitted user-tracking codes and the app's name to more than a dozen companies, essentially tagging individuals with their sexual orientation, according to the report, which was released Tuesday by the Norwegian Consumer Council, a government-funded nonprofit organization in Oslo.

Grindr also sent a user's location to multiple companies, which may then share that data with many other businesses, the report said. When The New York Times tested Grindr's Android app, it shared precise latitude and longitude information with five companies.

The researchers also reported that the OkCupid app sent a user's ethnicity and answers to personal profile questions — like "Have you used psychedelic drugs?" — to a firm that helps companies tailor marketing messages to users. The Times found that the OkCupid site had recently posted a list of more than 300 advertising and analytics "partners" with which it may share users' information.

"Any consumer with an average number of apps on their phone — anywhere between 40 and 80 apps — will have their data shared with hundreds or perhaps thousands of actors online," said Finn Myrstad, the digital policy director for the Norwegian Consumer Council, who oversaw the report.




A typical user who enables location tracking, for instance, may have that data shared with hundreds or thousands of companies, Mr. Myrstad said. Thomas Ekström for The New York Times

The report, "Out of Control: How Consumers Are Exploited by the Online Advertising Industry," adds to a growing body of research exposing a vast ecosystem of companies that freely track hundreds of millions of people and peddle their personal information. This surveillance system enables scores of businesses, whose names are unknown to many consumers, to quietly profile individuals, target them with ads and try to sway their behavior.

The report appears just two weeks after California put into effect a broad new consumer privacy law. Among other things, the law requires many companies that trade consumers' personal details for money or other compensation to allow people to easily stop the spread of their information.

In addition, regulators in the European Union are stepping up enforcement of their own data protection law, which prohibits companies from collecting personal information on religion, ethnicity, sexual orientation, sex life and other sensitive subjects without a person's explicit consent.

The Norwegian group said it filed complaints on Tuesday asking regulators in Oslo to investigate Grindr and five ad tech companies for possible violations of the European data protection law. A coalition of consumer groups in the United States said it sent letters to American regulators, including the attorney general of California, urging them to investigate whether the companies' practices violated federal and state laws.

In a statement, the Match Group, which owns OkCupid and Tinder, said it worked with outside companies to assist with providing services and shared only specific user data deemed necessary for those services. Match added that it complied with privacy laws and had strict contracts with vendors to ensure the security of users' personal data.

In a statement, Grindr said it had not received a copy of the report and could not comment specifically on the content. Grindr added that it valued users' privacy, had put safeguards in place to protect their personal information and described its data practices — and users' privacy options — in its privacy policy

The report examines how developers embed software from ad tech companies into their apps to track users' app use and real-life locations, a common practice. To help developers place ads in their apps, ad tech companies may spread users' information to advertisers, personalized marketing services, location data brokers and ad platforms.

The personal data that ad software extracts from apps is typically tied to a user-tracking code that is unique for each mobile device. Companies use the tracking codes to build rich profiles of people over time across multiple apps and sites. But even without their real names, individuals in such data sets may be identified and located in real life.

For the report, the Norwegian Consumer Council hired Mnemonic, a cybersecurity firm in Oslo, to examine how ad tech software extracted user data from 10 popular Android apps. The findings suggest that some companies treat intimate information, like gender preference or drug habits, no differently from more innocuous information, like favorite foods.

Among other things, the researchers found that Tinder sent a user's gender and the gender the user was looking to date to two marketing firms.

The researchers did not test iPhone apps. Settings on both Android phones and iPhones enable users to limit ad tracking.

The group's findings illustrate how challenging it would be for even the most intrepid consumers to track and hinder the spread of their personal information.

Grindr's app, for instance, includes software from MoPub, Twitter's ad service, which can collect the app's name and a user's precise device location, the report said. MoPub in turn says it may share user data with more than 180 partner companies. One of those partners is an ad tech company owned by AT&T, which may share data with more than 1,000 "third-party providers."

In a statement, Twitter said: "We are currently investigating this issue to understand the sufficiency of Grindr's consent mechanism. In the meantime, we have disabled Grindr's MoPub account."

AT&T declined to comment.

The spread of users' location and other sensitive information could present particular risks to people who use Grindr in countries, like Qatar and Pakistan, where consensual same-sex sexual acts are illegal.

This is not the first time that Grindr has faced criticism for spreading its users' information. In 2018, another Norwegian nonprofit group found that the app had been broadcasting users' H.I.V. status to two mobile app service companies. Grindr subsequently announced that it had stopped the practice.

The report's findings also raise questions about the extent to which businesses are complying with the new California privacy law. The law requires many companies that benefit from trading consumers' personal details to prominently post a "Do Not Sell My Data" option, allowing people to stop the spread of their information.

But Grindr's stance challenges that idea. By agreeing to its policy, its site says, users "are directing us to disclose" their personal information "and, therefore, Grindr does not sell your personal data."

Mr. Myrstad said many consumers were comfortable sharing their data with apps they trusted. "But this study clearly shows that many apps abuse that trust," he said. "Authorities need to enforce the rules we have, and if they are not good enough, we have to make better rules."