The Washington Post
Democracy Dies in Darkness

TECHNOLOGY

A priest's phone location data outed his private life. It could happen to anyone.

How an unregulated market for personal data is legal, and what it means for your privacy

By Heather Kelly

July 22, 2021 at 6:23 p.m. EDT

A Catholic priest allegedly downloaded a popular gay dating app onto his smartphone years ago, perhaps assuming it would keep his secret.

This week, Monsignor Jeffrey Burrill stepped down from his job as top administrator for the U.S. Conference of Catholic Bishops after a newsletter said it used his location data to determine he was using the Grindr app and frequenting gay bars.

What stands out about this particular incident isn't that it's improbable but that it's the exact worst-case scenario privacy experts have been warning about for a long time. Personal data is collected, sold and bought by a tangle of app developers, data brokers and advertising companies with little oversight. The biggest shock may be that it didn't happen sooner.

"This is the first instance that I know of, of this data being used by a journalistic entity to track a specific person and weaponize their private, secretly collected information against them," said Bennett Cyphers, a staff technologist at the Electronic Frontier Foundation, a digital rights organization. "This is exactly the kind of privacy threat advocates have been describing for years."

There is still much to be learned about how the priest's private data could have made the journey from his smartphone into the hands of a Catholic newsletter's writer. The newsletter, the Pillar, didn't name the source of the data or clarify how it obtained the revealing location information, which it says spanned three years. But the story implies it started with data that Grindr allegedly shared with advertising partners and data brokers in the past that was then legally sold by a data broker.

In a statement posted to Twitter defending the article and the anonymity it granted the data provider, method and funder, the Pillar's editor in chief, JD Flynn, said it weighed the balance between an individual's privacy and public interest, and was "confident in our deliberation." He added that "technology accountability has been an issue of importance among church leaders for quite some time."

issue of importance among church leaders for quite some time.

How anyone's information could end up for sale

Right now, your smartphone is likely filled with apps that are collecting details about you, including your age, gender, political leanings, GPS data or browsing habits.

Grindr and other apps have long shared this kind of information with third-party data brokers, which exist in a largely unregulated sweet spot between websites, apps and advertisers. The brokers gather the data from apps, then sell it on the open market to parties that use it for ad targeting, political profiling or even research. It's a well-established industry but one that doesn't typically draw this level of attention.

"Often the location data is used to determine what stores people visit. Things like sexual orientation are used to determine what demographics to target," said Ashkan Soltani, an independent researcher and a former chief technologist at the Federal Trade Commission. "People don't actually know or care that much that they're being targeted. Or it's used by nation state actors to surveil people, but that's not publicly talked about."

It's all above board, app companies have claimed, because the arrangement is spelled out in their privacy policies and there are precautions built in.

Experts say those precautions aren't enough. The data is typically stripped of the most obvious identifying information like a name, email or cell number. However, it still contains information that could reveal the person behind it, such as a device ID, an IP address or an advertising identifier. With the right outside information or a third-party service, so-called anonymous data can be de-anonymized, as the Pillar claims it did in the case of Burrill.

In this case, the Pillar says it "correlated a unique mobile device to Burrill" using his presence at his family lake house, meetings he attended and the USCCB staff residence and headquarters. It did not say how it collected that information. The Pillar says the data set it used was "commercially available app signal data" from a data vendor that included Grindr information, but it did not name the vendor or clarify if it bought the data directly from a broker or received it from another party.

In a 2013 paper, researchers found that as little as four pieces of data on average were enough to re-identify someone 95 percent of the time. Latanya Sweeney, a data privacy expert and professor at Harvard Kennedy School, showed how just a Zip code, age and gender could be used to identify patients in anonymous hospital data sets. Even something as simple as a person's work and home address could be enough to find a pattern strong enough to identify anonymous location data.

A 2020 study by the Norwegian Consumer Council found that Grindr and other apps were sharing personal data about their users with outside companies, including numerous data brokers. In Grindr's case, it also shared detailed location data, according to the Norwegian researchers.

In January this year, the Norwegian Data Protection Authority said it would fine Grindr $11.7 million for sharing data without users' consent. In its response, Grindr confirmed that it shared data, including a hashed device ID, age, gender and location information with advertisers, but claimed that it was done with consent from users and that the app had since updated its sharing policies.

"Historical data collection remains a problem," said Tor Erling Bjorstad, a security researcher at Mnemonic who was in charge of the Norwegian Consumer Council research report. "GPS position data collected in 2019 and earlier is still out there, and can still have explosive power."

Grindr said in a statement in response to the Pillar newsletter post on Tuesday that the alleged activities are "incredibly unlikely to occur." However, on Wednesday, it shared an updated statement saying that "we do not believe Grindr is the source of the data" and that the company had policies and systems in place to protect personal data. It did not specify what they were.

How you can protect yourself

What is stopping similar instances from happening to other people?

Very little, according to privacy experts.

"Consumers don't really have the tools to be able to protect themselves," said Serge Egelman, research director of the Usable Security and Privacy Group at the International Computer Science Institute. "Once the data leaves the device, there's no way of knowing what's actually going to happen to it, what other third parties will receive it. … There's no knowledge of how the data will be used by anyone."

Trying to fully protect your data would be a full-time job, and not something most smartphone owners could easily manage. To start, you'd need to comb through every privacy policy, manually opt out of any relevant sharing options for each app you download, use a virtual private network, or VPN, and maybe move somewhere with stronger consumer privacy protections like the European Union or even California.

In California, individuals have the right to ask companies not to sell their personal information, including anything under a pseudonymous identification like their device ID, if they know it. They can opt out of letting data brokers sell their information, one by one — an arduous task. In other locations, that process isn't available or is impossible.

There are some steps you can take to try to reduce your exposure, says EFF's Cyphers.

Download fewer smartphone apps in general and delete anything you don't use. Lock down the kinds of data the remaining apps are able to access, especially your location. Go into your phone's privacy settings and look up location sharing, where you should find a list of apps with access to your location. Both Android and iOS devices let you limit when an app can access your location. Always limit location access to while you're using the app or make the app ask each time, and never let an app continuously track your location in the background without an exceptionally good reason. Reset your advertising ID in your smartphone's settings.

If you're worried about someone knowing your browsing history, use a VPN, but be careful about which ones. (Cyphers says a VPN won't protect your location information as well.)

Ultimately, it's an overwhelming amount of work to ask of regular people. It's a problem that may require more serious intervention, such as privacy regulation or even stricter rules for apps from the smartphone makers

themselves.

“Time and time again, whenever the burden is on users to opt out of something, the vast amount of users are not going to opt out of that thing,” said Cyphers.