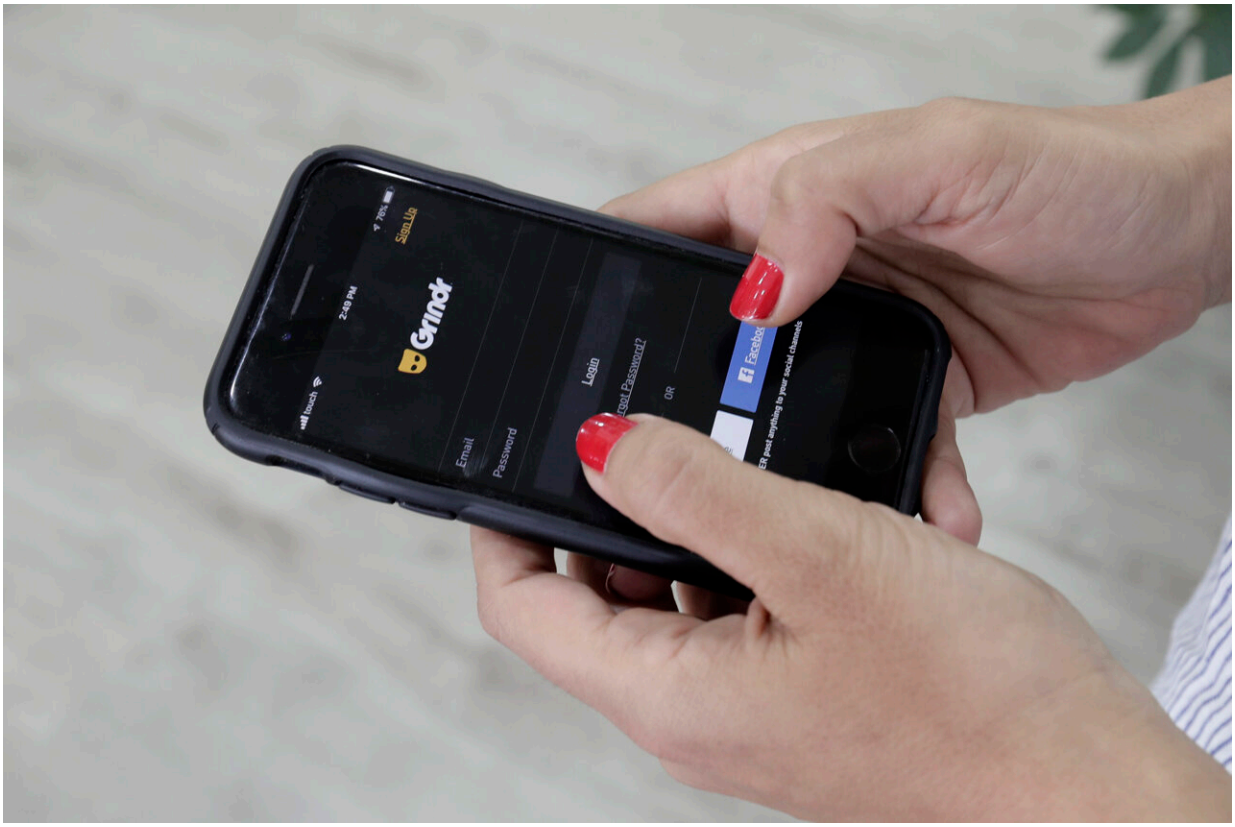
Priest outed via Grindr app highlights rampant data tracking

July 23 2021, by Matt O'brien and Frank Bajak



In this Wednesday, May 29, 2019 file photo, a woman looks at the Grindr app on her mobile phone in Beirut, Lebanon. With few rules in the U.S. guiding what companies can do with the vast amount of information they collect about what web pages people visit, the apps they use and where they carry their devices, there's little stopping similar spying activity targeting politicians, celebrities and just about anyone that's a target of another person's curiosity. Credit: AP Photo/Hassan Ammar, File

When a religious publication used smartphone app data to deduce the sexual orientation of a high-ranking Roman Catholic official, it exposed a problem that goes far beyond a debate over church doctrine and priestly celibacy.

With few U.S. restrictions on what companies can do with the vast amount of data they collect from web page visits, apps and location tracking built into phones, there's not much to stop similar spying on politicians, celebrities and just about anyone that's a target of another person's curiosity—or malice.

Citing allegations of "possible improper behavior," the U.S. Conference of Catholic Bishops on Tuesday announced the resignation of its top administrative official, Monsignor Jeffrey Burrill, ahead of a report by the Catholic news outlet The Pillar that probed his private romantic life.

The Pillar said it obtained "commercially available" location data from a vendor it didn't name that it "correlated" to Burrill's phone to determine that he had visited gay bars and private residences while using Grindr, a dating app popular with gay people.

"Cases like this are only going to multiply," said Alvaro Bedoya, director of the Center for Privacy and Technology at Georgetown Law School.

Privacy activists have long agitated for laws that would prevent such abuses, although in the U.S. they only exist in a few states, and then in varying forms. Bedoya said the firing of Burrill should drive home the danger of this situation, and should finally spur Congress and the Federal Trade Commission to act.

Privacy concerns are often construed in abstract terms, he said, "when it's really, 'Can you explore your sexuality without your employer firing you? Can you live in peace after an abusive relationship without fear?'"

Many abuse victims take great care to ensure that their abuser can't find them again.

As a congressional staffer in 2012, Bedoya worked on legislation that would have banned apps that let abusers secretly track their victims' locations through smartphone data. But it was never passed.

"No one can claim this is a surprise," Bedoya said. "No one can claim that they weren't warned."

Privacy advocates have been warning for years that location and personal data collected by advertisers and amassed and sold by brokers can be used to identify individuals, isn't secured as well as it should be and is not regulated by laws that require the clear consent of the person being tracked. Both legal and technical protections are necessary so that smartphone users can push back, they say.

The Pillar alleged "serial sexual misconduct" by Burrill—homosexual activity is considered sinful under Catholic doctrine, and priests are expected to remain celibate. The online publication's website describes it as focused on investigative journalism that "can help the Church to better serve its sacred mission, the salvation of souls."

Its editors didn't respond to requests for comment Thursday about how they obtained the data. The report said only that the data came from one of the data brokers that aggregate and sell app signal data, and that the publication also contracted an independent data consulting firm to authenticate it.

There are brokers that charge thousands of dollars a month for huge volumes of location data, some of which is marketed not just to advertisers but to landlords, bail bondsmen and bounty hunters, said John Davisson, senior counsel at the Electronic Privacy Information Center.

He said someone looking to "reverse engineer" a particular person's data from that bulk package could potentially get it from any of the many customers in the data chain.

"It is surprisingly and disturbingly cheap to obtain location data derived from mobile phones," Davisson said. "It's easy enough that a determined party can do it."

U.S. Sen. Ron Wyden, an Oregon Democrat, said the incident confirms yet again the dishonesty of an industry that falsely claims to safeguard the privacy of phone users.

"Experts have warned for years that data collected by advertising companies from Americans' phones could be used to track them and reveal the most personal details of their lives. Unfortunately, they were right," he said in a statement. "Data brokers and advertising companies have lied to the public, assuring them that the information they collected was anonymous. As this awful episode demonstrates, those claims were bogus—individuals can be tracked and identified."

Wyden and other lawmakers asked the FTC last year to investigate the industry. It needs "to step up and protect Americans from these outrageous privacy violations, and Congress needs to pass comprehensive federal privacy legislation," he added.

Norway's data privacy watchdog concluded earlier this year that Grindr shared personal user data with a number of third parties without legal basis and said it would impose a fine of $11.7 million (100 million Norwegian krone), equal to 10% of the California company's global revenue.

The data leaked to advertising technology companies for targeted ads included GPS location, user profile information as well as the simple

fact that particular individuals were using Grindr, which could indicate their sexual orientation.

Sharing such information could put someone at risk of being targeted, the Norwegian Data Protection Authority said. It argued that the way Grindr asked users for permission to use their information violated European Union requirements for "valid consent." Users weren't given the chance to opt out of sharing data with third parties and were forced to accept Grindr's privacy policy in its entirety, it said, adding that users weren't properly informed about the data sharing.

The advertising partners that Grindr shared data with included Twitter, AT&T's Xandr service, and other ad-tech companies OpenX, AdColony and Smaato, the Norwegian watchdog said. Its investigation followed a complaint by a Norwegian consumer group that found similar data leakage problems at other popular dating apps such as OkCupid and Tinder.

In a statement, Grindr called The Pillar's report an "unethical, homophobic witch hunt" and said it does "not believe" it was the source of the data used. The company said it has policies and systems in place to protect personal data, although it didn't say when those were implemented. The Pillar said the app data it obtained about Burrill covered parts of 2018, 2019 and 2020.