Pay to Pray: The Privacy Pitfalls of Faith-based Mobile Apps

The aim of Disinfo Radar's Rapid Response Briefs is to identify new and noteworthy disinformation technologies, tactics and narratives. Such cases may include the identification of a new technology that may have harmful uses.

Background

With their flocks forced to stay home and pastors, priests and imams made to preach via Zoom during the COVID-19 pandemic, an opportunity presented itself akin to what venture capitalist Katherine Boyle has called a "holy trinity": "isolated people hungry for attachment, religions desperate for growth in an online world, and technology investors searching for the consumer niches yet to digitize."

The resulting groundswell of faith-based mobile apps was quickly endorsed by some of Silicon Valley's best-known investors, including Peter Thiel and Andreessen Horowitz. Venture capital for religious mobile apps grew from USD 6.1 million in 2016 to USD 175.3 million in 2021, according to market research firm PitchBook Data, and success stories like Muslim Pro and Pray.com currently boast tens of millions of downloads.

Despite the altruistic claims of their founders, investigations into several faith-based apps reveal that many harvest sensitive information and sell it to untransparent third-party vendors. In some cases, sensitive information about religious communities reportedly ends up in the hands of governments.

Such exploitative practices have the potential to infringe upon the privacy of vulnerable communities and provide malicious actors with the information they need to craft targeted disinformation campaigns. These dangers urgently need to be addressed by both regulators and tech gatekeepers.

What Are Faith-based Mobile Apps?

The best-known faith-based apps target Christian practitioners, and many have been on the market for nearly a decade. The pandemic provided the impetus for these start-ups to scale up their operations to meet the demand of would-be churchgoers forced to isolate at home.

Market leaders such as Pray.com, Hallow and Glorify, though targeting different denominations, have similar offerings and business models. For a monthly subscription, users receive customised daily prayers, daily meditations and, in the case of Pray.com, recordings of celebrities reading Bible verses. Non-Christian contemporaries, such as Muslim Pro, remind users when to pray throughout the day and calibrate the direction of Mecca based on a user's location.

How and to Whom are they Selling Data?

The creators of these apps claim they are not in the business of selling data and that, instead, they are leading a digital religious revival. A number of investigations over the past year, in addition to the apps' own privacy policies, provide evidence to the contrary.

One example is Pray.com. An audit by privacy researcher Zach Edwards, conducted as part of a BuzzFeed investigation, found that data about the content users viewed within the app – including content related to prayer posts – was subsequently sold to companies like Facebook, as well as to third-party vendors specialised in crafting targeted advertising. The Mozilla Foundation's review of the app's privacy policy and tech framework revealed that it can access the camera, microphone and location of a user's mobile phone, and even its flashlight.

These third-party vendors can be one of a host of actors, including government agencies. A recent Motherboard investigation tracked movement data from Muslim Pro sold to third parties and discovered that a United States agency tasked with counterterrorism and reconnaissance is a buyer. The vendor in question reported that it tracks some 25 million devices in the United States every month and 40 million around the world, including in the European Union, which has the world's strictest data-privacy regime.

Many developers claim to be unaware of the ultimate buyers of user data. They are often paid a per-user rate from vendors to embed into their apps a unique software development kit (SDK), a code bundle that can aid app functionality, but can also collect users' data and transmit it back to the vendor.

A study for the Australian Competition and Consumer Commission (ACCC) reported in 2020 that, of 1,000 apps it tested, many of the most popular SDKs were designed to collect user information for advertising purposes – 92% contained Google SDKs and 61% contained those for Facebook. Despite opt-in data-privacy rules for users and app-store policies, dozens of apps transmitted Wi-Fi MAC addresses to vendors, which are linked to hardware and can be used for

long-term tracking.

In 2015, Google's terms of use prohibited Android developers from selling apps with such data-collection practices on the Play Store. But since the Android operating system is open source, compared to Apple's tightly controlled iOS, many security and privacy gaps remain.

What's the Threat?

Regardless of whether data is funnelled to third-party vendors or leaked to the masses, it can result in "surveillance targeting," where disinformation is packaged into social media advertising and precisely targeted at groups for whom the false messaging will be most salient.

In recent years, some social media platforms have sought to track and ban such disinformation tactics, especially as they relate to pandemic disinformation or false claims spread by the accounts of politicians. But the success of such policies remains a black box. Most platforms publish little information about the enforcement of their targeting policies and do not provide researchers with the ad APIs needed to uncover how private information shared through such apps increasingly shapes the disinformation tactics and narratives of malicious actors.

Researchers with the Brookings Institution have pointed out that this type of "surveillance capitalism" can also result in the persecution of vulnerable communities Faith-based, as well as popular gay dating, menstrual cycle tracking and children's educational mobile applications, have all been linked to dubious sharing practices that resulted in either private or government persecution, surveillance or arrests.

Recommended Responses:

- Require SDK compliance testing for newly developed apps that deal with extremely personal user information (e.g., faith-based apps). This should especially be the case for Google's Play Store, which reports indicate has the most security holes, allowing for dubious data-sharing and surveillance targeting to continue under the radar.

- Create transparency registers for third-party data vendors to ensure better oversight of their business models.

- Grant researchers and journalists greater access to platforms' advertisement APIs, so they can better evaluate how extremely private information shared over faith-based and other daily-use apps shapes disinformation tactics and narratives.

DISINFO RADAR

Date: October 2022

This Rapid Response Brief was written by Democracy Reporting International's Austin Davis and is part of DRI's Disinfo Radar project funded by the German Federal Foreign Office. Its contents do not necessarily represent the position of the German Federal Foreign Office.

About Democracy Reporting International

DRI is an independent organisation dedicated to promoting democracy worldwide. We believe that people are active participants in public life, not subjects of their governments. Our work centres on analysis, reporting and capacity-building. For this, we are guided by the democratic and human rights obligations enshrined in international law. Headquartered in Berlin, DRI has offices in Lebanon, Libya, Myanmar, Pakistan, Sri Lanka, Tunisia, and Ukraine.