Gabriel Hongsdusit

UPDATE: Life360 announced that it will stop sales of precise location data to the dozen or so data brokers it had been working with, and will now sell only precise location data to Arity and "aggregated" location data to PlacerAI.

Life360, a popular family safety app used by 33 million people worldwide, has been marketed as a great way for parents to track their children's movements using their cellphones. The Markup has learned, however, that the app is selling data on kids' and families' whereabouts to approximately a dozen data brokers who have sold data to virtually anyone who wants to buy it.

Through interviews with two former employees of the company, along with two individuals who formerly worked at location data brokers Cuebiq and X-Mode, The Markup discovered that the app acts as a firehose of data for a controversial industry that has operated in the shadows with few safeguards to prevent the misuse of this sensitive information. The former employees spoke with The Markup on the condition that we not use their names, as they are all still employed in the data industry. They said they agreed to talk because of concerns with the location data industry's security and privacy and a desire to shed more light on the opaque location data economy. All of them described Life360 as one of the largest sources of data for the industry.

"We have no means to confirm or deny the accuracy" of whether Life360 is among the largest sources of data for the industry, Life360 founder and CEO Chris Hulls said in an emailed response to questions from The Markup. "We see data as an important part of our business model that allows us to keep the core Life360 services free for the majority of our users, including features that have improved driver safety and saved numerous lives."

A former X-Mode engineer said the raw location data the company received from Life360 was among X-Mode's most valuable offerings due to the sheer volume and precision of the data. A former Cuebiq employee joked that the company wouldn't be able to run its marketing campaigns without Life360's constant flow of location data.

The Markup was able to confirm with a former Life360 employee and a former employee of X-Mode that X-Mode—in addition to Cuebiq and Allstate's Arity, which the company discloses in its privacy policy—is among the companies that Life360 sells data to. The former Life360 employee also told us Safegraph was among the buyers, which was confirmed by an email from a Life360 executive that was viewed by The Markup. There are potentially more companies that benefit from Life360's data based on those partners' customers.

Hulls declined to disclose a full list of Life360's data customers and declined to confirm that Safegraph is among them, citing confidentiality clauses, which he said are in the majority of its business contracts. Data partners are only publicly disclosed when partners request transparency or there's "a particular reason to do so," Hulls said. He did confirm that X-Mode buys data from Life360 and that it is one of "approximately one dozen data partners." Hulls added that the company would be supportive of legislation that would require public disclosure of such partners.

X-Mode, SafeGraph, and Cuebiq are known location data companies that supply data and insights gleaned from that data to other industry players, as well as customers like hedge funds or firms that deal in targeted advertising.

Cuebiq spokesperson Bill Daddi said in an email that the company doesn't sell raw location data but provides access to an aggregated set of data through its "Workbench" tool to customers including the Centers for Disease Control and Prevention. Cuebiq, which receives raw location data from Life360, has publicly disclosed its partnership with the CDC to track "mobility trends" related to the COVID-19 pandemic.

"The CDC only exports aggregate, privacy-safe analytics for research purposes, which completely anonymizes any individual user data," Daddi said. "Cuebiq does not sell data to law enforcement agencies or provide raw data feeds to government partners (unlike others, such as X-Mode and SafeGraph)."

X-Mode has sold location data to the U.S. Department of Defense, and SafeGraph has sold location data to the CDC, according to public records.

X-Mode and SafeGraph didn't respond to requests for comment.

The Life360 CEO said that the company implemented a policy to prohibit the selling or marketing of Life360's data to any government agencies to be used for a law enforcement purpose in 2020, though the company has been selling data since at least 2016.

"From a philosophical standpoint, we do not believe it is appropriate for government agencies to attempt to obtain data in the commercial market as a way to bypass an individual's right to due process," Hulls said.

The policy also applies to any companies that Life360's customers share data with, he said. Hulls said the company maintains "an open and ongoing dialogue" with its customers to ensure they comply with the policy, though he acknowledged that it was a challenge to monitor partners' activities.

Life360 discloses in the fine print of its privacy policy that it sells the data it gleans from app users, but Justin Sherman, a cyber policy fellow at the Duke Tech Policy Lab, said people are probably not aware of how far their data can travel.

The company's privacy policy notes Life360 "may also share your information with third parties in a form that does not reasonably identify you directly. These third parties may use the de-identified information for any purpose."

"Families probably would not like the slogan, 'You can watch where your kids are, and so can anyone who buys this information,' " Sherman said.

Two former Life360 employees also told The Markup that the company, while it states it anonymizes the data it sells, fails to take necessary precautions to ensure that location histories cannot be traced back to individuals. They said that while the company removed the most obvious identifying user information, it did not make efforts to "fuzz," "hash," aggregate, or reduce the precision of the location data to preserve privacy.

Hulls said that all of Life360's contracts prohibit its customers from re-identifying individual users, along with other privacy and safety protective practices. He said that Life360 follows "industry best practices" for privacy and that only certain customers like Cuebiq receive raw location data. The former X-Mode engineer said that the company also received raw data from Life360. The company relies on its customers to obfuscate that data based on their specific applications, Hulls added.

Do you work at Life360, X-Mode or any other company that buys or sells location data?

We'd like to speak with you. You can reach out securely on Signal at 646-355-8306 or email keegan@themarkup.org.

"Some of our data partners receive hashed data and some do not based on how the data will be used," the Life360 founder said.

Meanwhile, selling location data has become more and more central to the company's health as it's struggled to achieve profitability. In 2016, the company made $693,000 from selling data it collected. In 2020, the company made $16 million—nearly 20 percent of its revenue that year—from selling location data, plus an additional $6 million from its partnership with Arity.

While still reporting a loss of $16.3 million last year, the company is expanding its business to include other "digital safety" products, rolling out data breach alerts, credit monitoring, and identity-theft-protection features. Publicly traded on the Australian Securities Exchange with plans to go public in the U.S., Life360 has also acquired companies that expand its tracking—and potentially its data-gathering capacity. In 2019, the company purchased ZenScreen, a family screen-time monitoring app. And in April, it purchased the wearable location device company Jiobit, aimed at tracking younger children, pets, and seniors, for $37 million. Hulls said Life360 has no plans to sell data from Jiobit devices or its digital safety services.

On Nov. 22, Life360 also announced plans to buy Tile, a tracking device company that helps find lost items. Hulls said the company doesn't have plans to sell data from Tile devices.

"I'm sure there are lots of families who do find very real comfort in an application like this, and that's valid," Sherman said. "That doesn't mean that there aren't ways that other people are harmed with this data. It also doesn't mean that the family couldn't be harmed with the data in ways that they're not aware of, such as that location data being used to target ads [or] used by insurance companies to figure out where they're traveling and increase their rates."

Hulls said that Life360 doesn't share users' private information with insurers in ways that could affect insurance rates.

The Data Pipeline

Life360's app allows the user to see the precise, real-time location of friends or family members, including the speed at which they are driving and the battery level on their devices.

Marketed as a safety app, Life360 is popular among parents who want to track and supervise their kids from afar. The app offers much of the functionality of Apple's built-in location-sharing features, but it includes emergency safety features such as an SOS button and vehicle crash detection. The company says these features have saved lives.

But Life360's location-based features are also sources of data points for a growing, multibillion-dollar industry that trades in location data gathered from mobile phones. Advertisers, government agencies, and investors are willing to spend hundreds of thousands of dollars for location data and the insights that can be derived from it.

While children can use the app (with parental consent), Life360's policy states that the company doesn't sell data on any users under 13. The Children's Online Privacy Protection Rule (better known as "COPPA") creates restrictions on digital services used by children under 13, and Life360 has detection methods like requiring a scan of a parent's ID for underage users. Life360 does "disclose" younger children's information to third parties "as needed to analyze and detect driving behavior data, perform analytics or otherwise ,[sic] support the features and functionality of our Service," according to its privacy policy, but not "for marketing or advertising purposes."

Marketers use location data to target ads to people near businesses, while investors buy data to determine popularity based on foot traffic. Government agencies have bought location data to track movement patterns and in one case to support "Special Operations Forces mission requirements overseas."

"It sounds like the company's pointing to a couple of cases where, sure, they helped somebody, they were able to do something good," Sherman said. "But then they will not talk about all of the other cases where the buying and selling of this data is potentially very harmful."

In July, a high-ranking Catholic priest resigned after a Catholic news outlet outed him by using location data from the gay dating app Grindr linked to his device. The data was obtained by an unknown vendor, and the report claimed to show that the priest frequented gay bars. There is no indication that Life360 was involved in this incident.

Grindr, like other apps that feed data into this industry, is required to ask for location permissions when a user first opens the app.

"We are not aware of any instance where our data has been traced back to individuals via our data partners," Hulls said. "Furthermore, our contracts contain language specifically prohibiting any reidentification, and we would aggressively take action against any breach of this term."

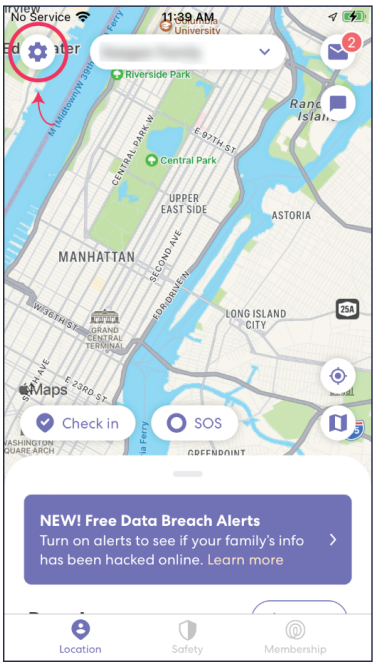
In Life360's case, because of how the app works, it asks for the broadest location permissions possible for functional purposes. Many apps that use location data allow users to grant access only while it's in use. Because Life360 is for tracking whereabouts in real time, the app asks for location data at all times—and does not function unless that permission is turned on.

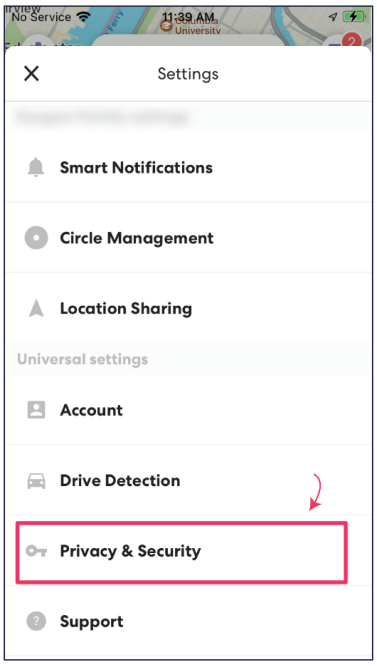
A disclaimer appears in smaller print at the bottom of the permissions screen: "Your location data may be shared with Partners for the purposes of crash detection, research, analytics, attribution and tailored advertising." Users can disable the sale of their location data in the privacy settings, though that setting is not disclosed in or part of the prompt.

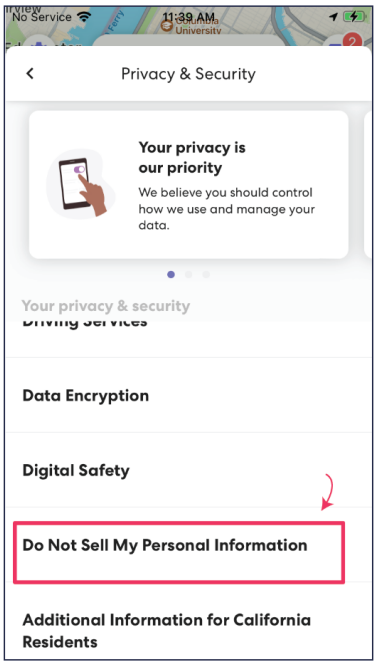
Life360's Hulls said that millions of its users have used this feature to opt out of their data being sold.

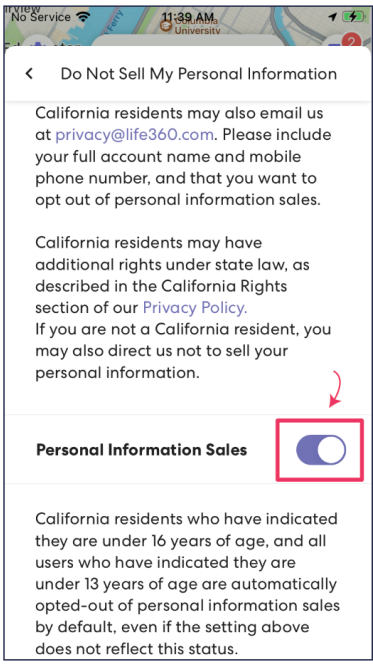
How to Disable the Sale of Your Location Data in the Life360 App

Tap on the gear icon for "Settings" **2. Tap on "Privacy & Security"** **3. Tap on "Do Not Sell My Personal Information"** **4. Toggle the button next to "Personal Information Sales" to the off position**









Source: Life360 app

For those who have not opted out, their Life360 data may be shared with the company's partners within 20 minutes of being recorded, a former Life360 employee said.

Hulls said this description was "directionally accurate," saying it only applied to certain partners and use cases.

"For example, some use cases, like road traffic probing, which powers travel time estimates in automotive navigation systems and GPS apps, require very fresh data," he said.

Privacy researchers and app store operators often look for data brokers' code in apps for signs of an app sending data off to third parties. But Life360 collects its data directly from the app and provides it to data brokers through its own servers.

Apple's and Google's app stores have no way of detecting this transfer of location data to a third party. "It makes sense to send this data directly from the server side from the app vendor so it can never be traced or observed by anyone," said Wolfie Christl, a researcher who investigates digital tracking.

Hulls said Life360's method of providing data through its own servers wasn't an intentional effort to evade detection from researchers and app stores.

"This is completely unrelated. We have our own proprietary sensor technology, which we started building in 2008 well before the emergence of the data industry, and we avoid using SDKs that could have a negative battery impact or other interplay with our own sensor technology," he said.

Google didn't comment on why Life360 was able to sell data this way despite its policy against selling location data. Apple spokesperson Adam Dema responded with a link to Life360's privacy policy but didn't comment about the company's data sales to companies like SafeGraph and X-Mode.

Hulls said Life360 de-identifies the data it sells, which can include a device's mobile advertising ID, IP address, and latitude and longitude coordinates collected by Life360's app.

Hulls clarified that "de-identification" involves removing usernames, emails, phone numbers, and other types of identifiable user information before the data is shared with Life360's customers. The data sold still includes a device's mobile advertising ID and latitude and longitude coordinates.

Even without names or phone numbers, researchers have repeatedly demonstrated how "anonymized" location data can easily be connected to the people from whom it came.

And privacy experts note that mobile advertising IDs are more valuable than identifiers like names.

"This code can be used to track and follow you across many life situations," Christl said. "As such, it is a much better identifier than a name."

Controversial Partners

The location data industry operates largely out of public view and with little oversight or regulation. Some of Life360's partners have faced controversy in the past over how they handle data and privacy.

Started in 2013 as Drunk Mode, a novelty app that "prevents users from drunk dialing," X-Mode was reportedly banned from the big app stores after Vice's Motherboard reported that the company was selling location data from Muslim prayer apps like Muslim Pro to U.S. government contractors associated with national security, raising concerns about unconstitutional government surveillance.

Public records show that X-Mode received at least $423,000 from the U.S. Air Force and the Defense Intelligence Agency for location data between 2019 and 2020. The company also sold data on Americans in profiled sets, like people who were drivers or likely to shop at department stores, according to Motherboard.

In August, X-Mode was purchased by intellectual property intelligence firm Digital Envoy and rebranded as Outlogic.

In response to the backlash over X-Mode's selling location data to defense contractors, its new owners said the company would stop selling U.S. location data to such companies.

"We cannot comment on the practices of another company or what that company does with data it receives from other sources," Hulls said. "However, Life360 has worked closely with X-Mode to ensure that X-Mode and all of its data customers do not sell data originating from Life360 to law enforcement agencies or to any government agency to be used for a law enforcement purpose."

SafeGraph is one of the biggest firms in the location data business, and its investors include venture capitalist Peter Thiel; Prince Turki Al Faisal Al Saud, former head of Saudi intelligence; and Life360's chief business officer, Itamar Novick.

The company specializes in data that associates places of interest with raw coordinates, adding a layer of meaning to the raw location data that the company ingests. SafeGraph was identified as not just a customer of Life360's data but also a major partner in an email from a Life360 executive that was viewed by The Markup.

In April, as first reported by Motherboard, SafeGraph was awarded a $420,000 contract to sell data to the Centers for Disease Control described as "Data Gathering and Reporting." The Washington Post also reported that SafeGraph shared billions of phone location records with the D.C. Department of Health through its spinoff company Veraset.

The company openly sells location data on Amazon's data marketplace, including a $240,000 yearly subscription to data on people across the U.S. Veraset has boasted of selling location data for purposes including marketing, real estate, investing, and city planning.

Sen. Ron Wyden has flagged SafeGraph as a "data broker of concern" to Google, Wyden's chief communications officer, Keith Chu, said in an email. The Democrat from Oregon has made multiple attempts to speak with SafeGraph to learn more about how the company obtains, sells, and shares Americans' location data, but the company never responded, Chu said.

Cuebiq also worked with the Centers for Disease Control, with a $208,000 contract awarded in June for aggregated location data, according to public records.

The CDC didn't respond to requests for comment.

During the beginning of the coronavirus pandemic, Cuebiq became a main source of location data for news outlets looking to report on people's movements after cities and states issued stay-at-home orders. Outlets including The New York Times and NBC News received location data from Cuebiq for their analyses.

It's been suggested that location data brokers like Cuebiq are using the pandemic to improve their public reputation by presenting themselves as tools for public health rather than as mechanisms for surveillance.

Cuebiq's Daddi said the company's data has helped in the aftermath of natural disasters and public health crises.

Safety vs. Privacy

Life360 has positioned itself as "the leading digital safety brand for families." But experts say families who use it are not necessarily thinking about their digital security.

"An app that claims to be a family safety service selling exact location data to several other companies, this is a total disaster," Christl said. "It would be a problem if it's any other app, and it's even more a problem when it's an app that claims to be a family safety service."

Life360 has faced concerns over privacy in the past. In mid-2020, teens, displeased at the privacy invasion of an app that allowed their parents to minutely track their movements, took to TikTok to encourage their peers to bomb the app with negative reviews. Over the course of a month, the app received more than a million one-star reviews, driving the average rating down from 4.6 to 2.7 stars.

Hulls responded by adding a "bubbles" feature that shows parents a more vague location of their child (but still allows parents to see exact locations with an additional step). He also recruited and paid teens to hawk the app on TikTok, resulting in a "viral surge in downloads," according to the company.

Those teens, however, were likely not aware that their parents were hardly the only ones privy to data on their movements.

Samira Madi, an 18-year-old student in Texas, started using Life360 when she was 15. She didn't have a problem with the company sharing her location data for marketing and advertising purposes, which the company readily disclosed.

After learning about who Life360 was selling data to, and the scale it was sold at, Madi felt that the company crossed a line.

“I had no idea it would be passed around this way,” Madi said in an email. “This concerns me because I would not want my location data to possibly be sold to people with ill intentions.”