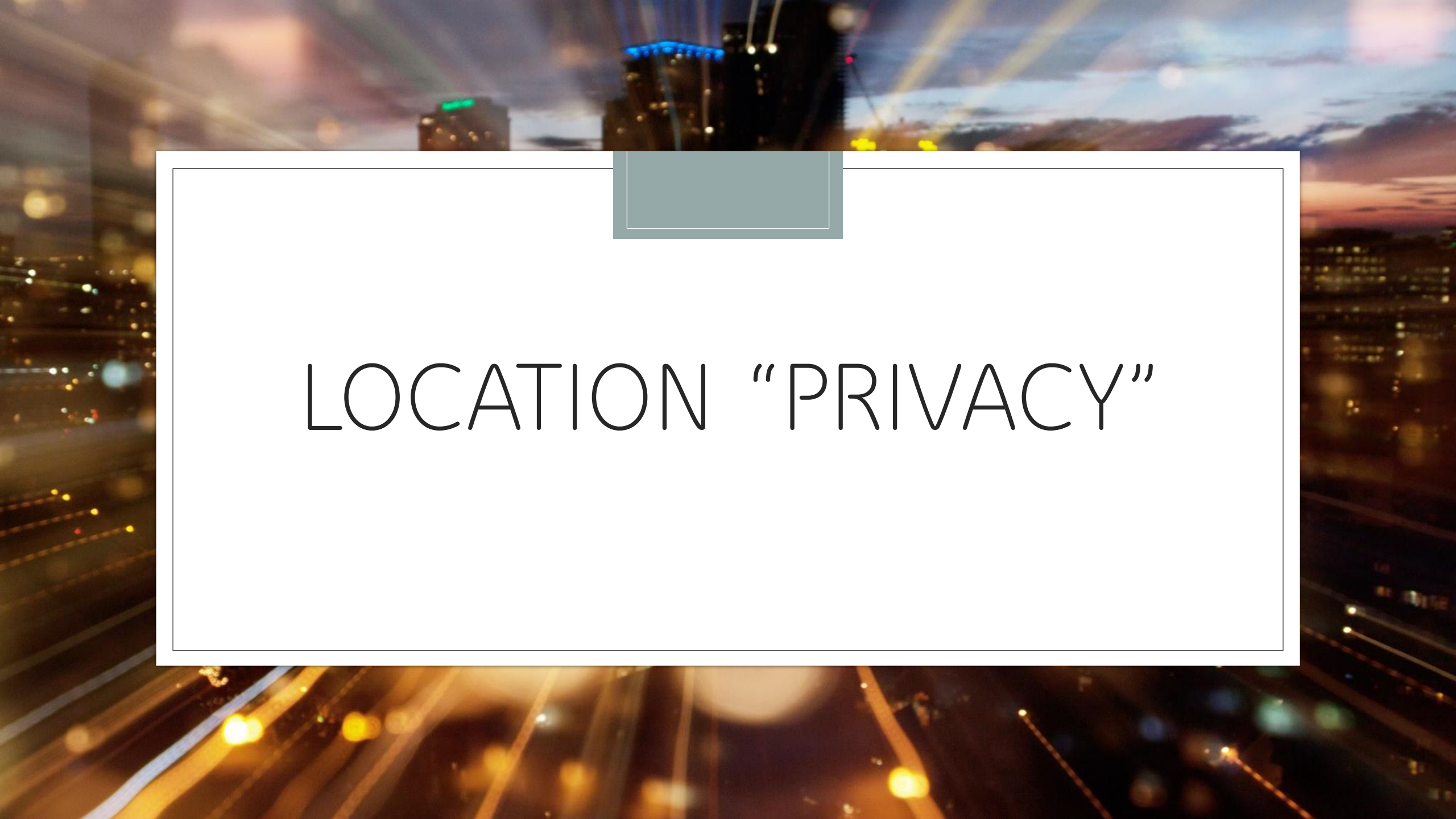


LOCATION “PRIVACY”

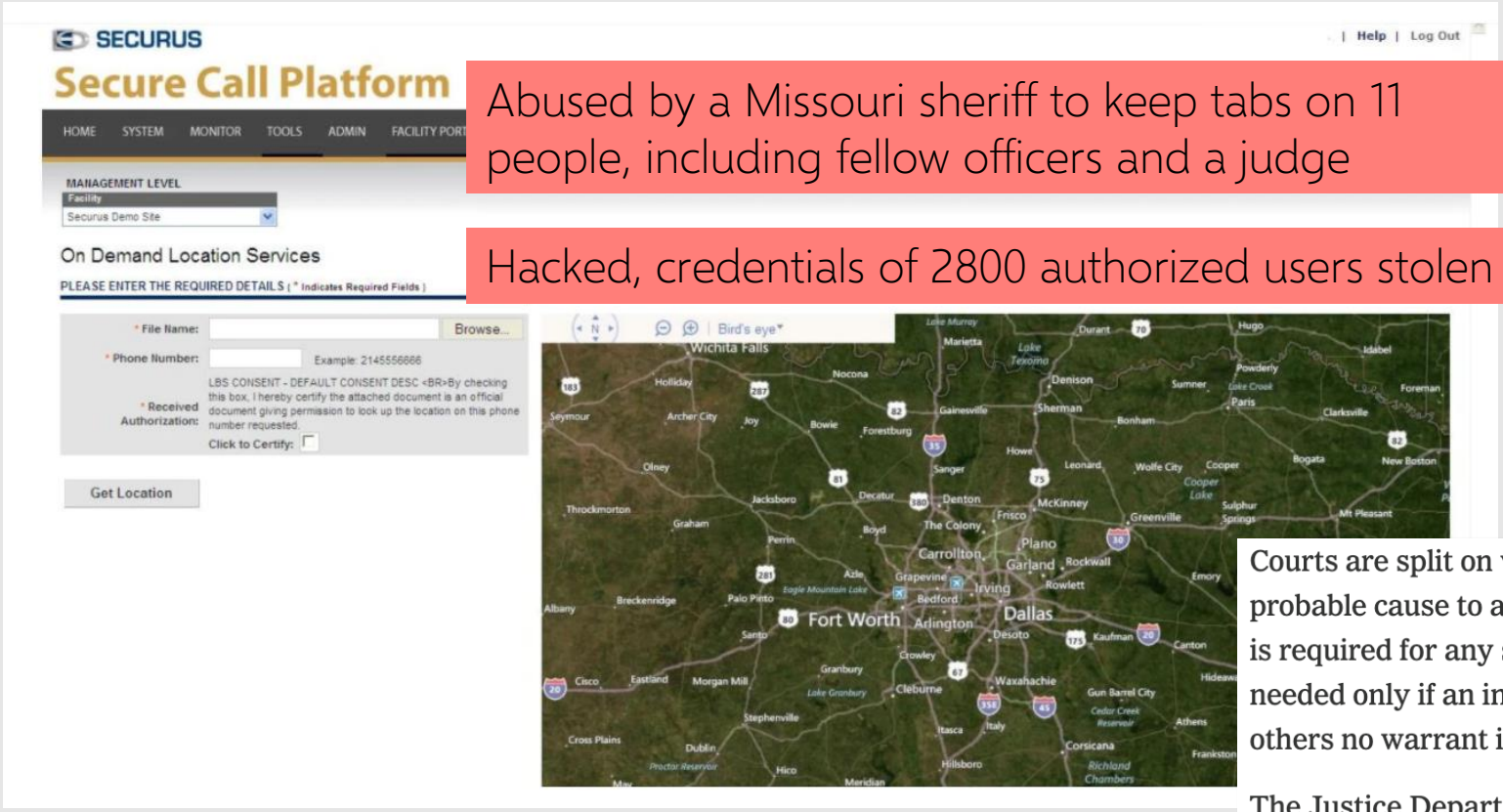
The Privacy Scandal That Should Be Bigger Than Cambridge Analytica

Wireless carriers are sharing your real-time location with shady third parties—and a bug lets anyone use that data to track you.

- Four largest US wireless carriers share location-tracking data with third parties, including a "location aggregator" called LocationSmart
- LocationSmart shares with 3CInteractive, a mobile marketer
- 3CInteractive shares with Securus, a prison phone provider

As long as they are following their own privacy policies, carriers "are largely free to do what they want with the information they obtain, including location information, as long as it's unrelated to a phone call," said Albert Gidari, the consulting director of privacy at the Stanford Center for Internet and Society and a former technology and telecommunications lawyer. Even when the phone is not making a call, the system receives location data, accurate within a few hundred feet, by communicating with the device and asking it which cellphone towers it is near.

https://www.nytimes.com/2018/05/10/technology/cellphone-tracking-law-enforcement.html
https://slate.com/technology/2018/05/the-locationsmart-scandal-is-bigger-than-cambridge-analytica-heres-why-no-one-is-talking-about-it.html



Abused by a Missouri sheriff to keep tabs on 11 people, including fellow officers and a judge

Hacked, credentials of 2800 authorized users stolen

Real-time cellphone locator for law enforcement and corrections officials

Requires users to upload a warrant or affidavit but does not "conduct any review of surveillance requests"

Courts are split on whether investigators need a warrant based on probable cause to acquire location data. In some states, a warrant is required for any sort of cellphone tracking. In other states, it is needed only if an investigator wants the data in real time. And in others no warrant is needed at all.

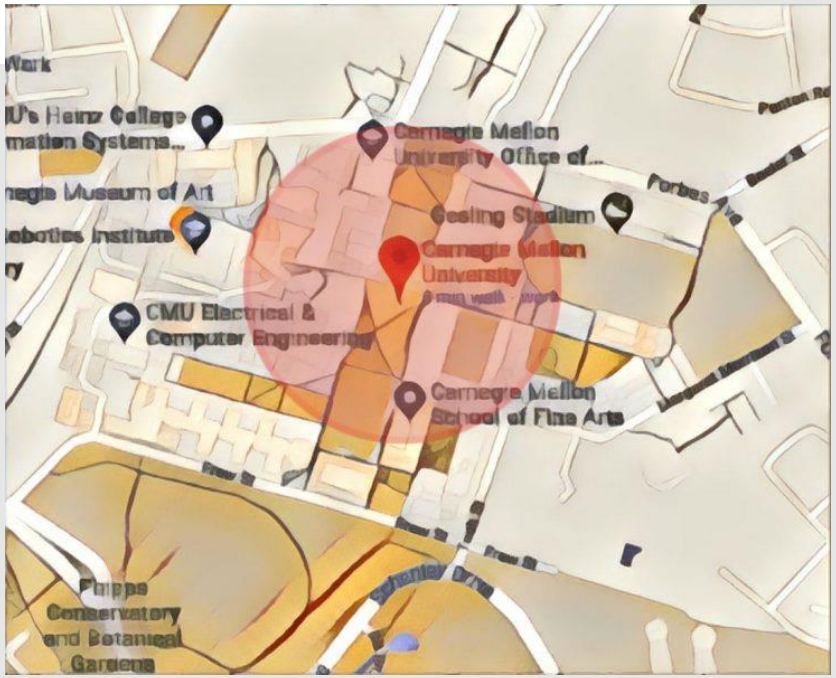
The Justice Department has said its policy is to get warrants for real-time tracking. The Supreme Court has ruled that putting a GPS tracker on a car counts as a search under the Fourth Amendment, but this was because installing the device involved touching a person's property — something that doesn't happen when a cellphone is pinged.

https://www.nytimes.com/2018/05/10/technology/cellphone-tracking-law-enforcement.html

It gets worse. A Carnegie Mellon researcher poking around on LocationSmart's website found that he could use a free trial service to instantly pinpoint the location of, well, just about anyone with a mobile phone and wireless service from one of those major carriers. He did this without any permission or credentials, let alone a warrant.

The reaction from the mainstream media and the public has been as muted as the reaction to Cambridge Analytica was explosive. Even tech sites have devoted relatively little coverage to the story. (Slate hasn't covered it either, until now.) Why might that be?

I have a theory—one that started as a hypothesis early on in the Cambridge Analytica scandal. It's that the outrage over the Cambridge Analytica story was never primarily about users' privacy or about Facebook's mishandling of users' data. It was about how that data was then used—purportedly, to help elect Donald Trump.

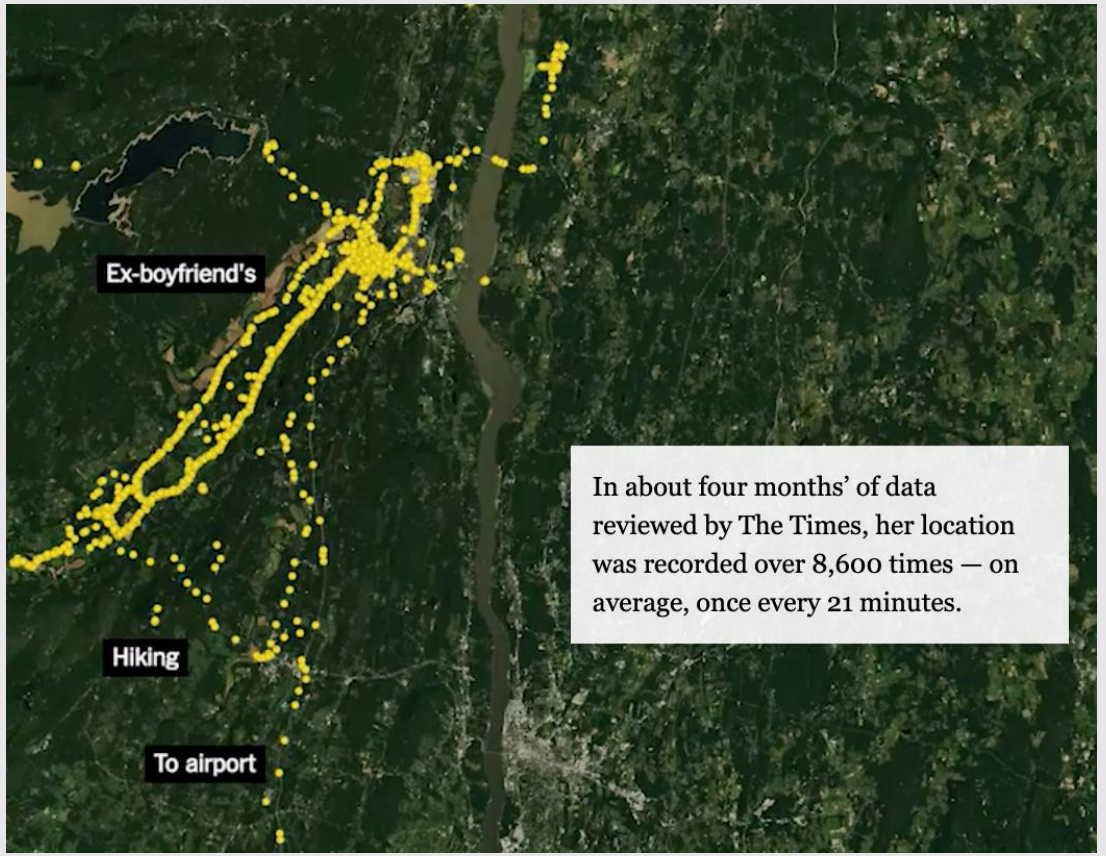


https://slate.com/technology/2018/05/the-locationsmart-scandal-is-bigger-than-cambridge-analytica-heres-why-no-one-is-talking-about-it.html

Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret

At least 75 companies receive anonymous, precise location data from apps whose users enable location services to get local news and weather or other information, The Times found. Several of those businesses claim to track up to 200 million mobile devices in the United States — about half those in use last year. The database reviewed by The Times — a sample of information gathered in 2017 and held by one company — reveals people's travels in startling detail, accurate to within a few yards and in some cases updated more than 14,000 times a day.

https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html



https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html

By Michael H. Keller | Imagery by Google Earth

By Michael H. Keller | Satellite imagery by Mapbox and DigitalGlobe

https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html

A Question of Awareness

Companies that use location data say that people agree to share their information in exchange for customized services, rewards and discounts. Ms. Magrin, the teacher, noted that she liked that tracking technology let her record her jogging routes.

> But it is easy to share information without realizing it. Of the 17 apps that The Times saw sending precise location data, just three on iOS and one on Android told users in a prompt during the permission process that the information could be used for advertising. Only one app, GasBuddy, which identifies nearby gas stations, indicated that data could also be shared to "analyze industry trends."

Brian Wong, chief executive of [illegible] anonymous data from some of [illegible] permission to use and share their data. "You are receiving these services for free because advertisers are helping monetize and pay for it," he said, adding, "You would have to be pretty oblivious if you are not aware that this is going on."

https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html

A Question of Awareness

Even industry insiders acknowledge that many people either don't read those policies or may not fully understand their opaque language. Policies for apps that funnel location information to help investment firms, for instance, have said the data is used for market analysis, or simply shared for business purposes.

"Most people don't know what's going on," said Emmett Kilduff, the chief executive of Eagle Alpha, which sells data to financial firms and hedge funds. Mr. Kilduff said responsibility for complying with data-gathering regulations fell to the companies that collected it from people.

https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html

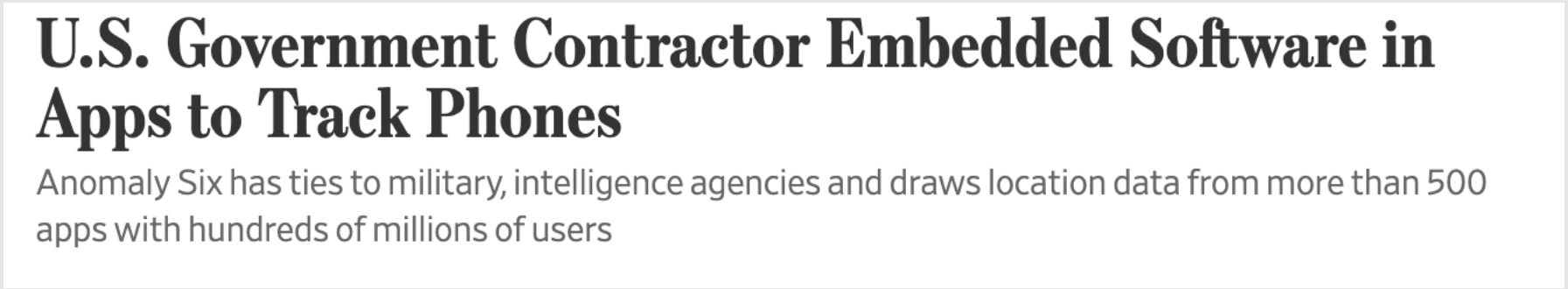
- Location-collecting apps publish aggregate statistics
  - Example: “heat maps” of user’s fitness activities
- … reveal locations of secret military objects, home addresses of military and intelligence officers

Strava ”heat maps”

Publicly shared user profiles in Polar

https://slate.com/technology/2018/07/fitness-tracking-apps-strava-polar-privacy-flaws-show-the-cost-of-sharing-activity-data.html

- SDK maker pays app publishers to embed SDK into their apps
- Presence of SDKs not disclosed in privacy policies
- SDK has same permissions as app, collects data



U.S. Government Contractor Embedded Software in Apps to Track Phones

Anomaly Six has ties to military, intelligence agencies and draws location data from more than 500 apps with hundreds of millions of users

https://www.wsj.com/articles/u-s-government-contractor-embedded-software-in-apps-to-track-phones-11596808801

- Anonymous cellphone location profiles used to find military sites
  - Look for phones located in government buildings, embassies, etc., then search for other locations they visited
- Includes cellphone location data drawn from advertising industry

Academic Project Used Marketing Data to Monitor Russian Military Sites

Commercially available location data is increasingly used for sensitive surveillance by researchers, government agencies

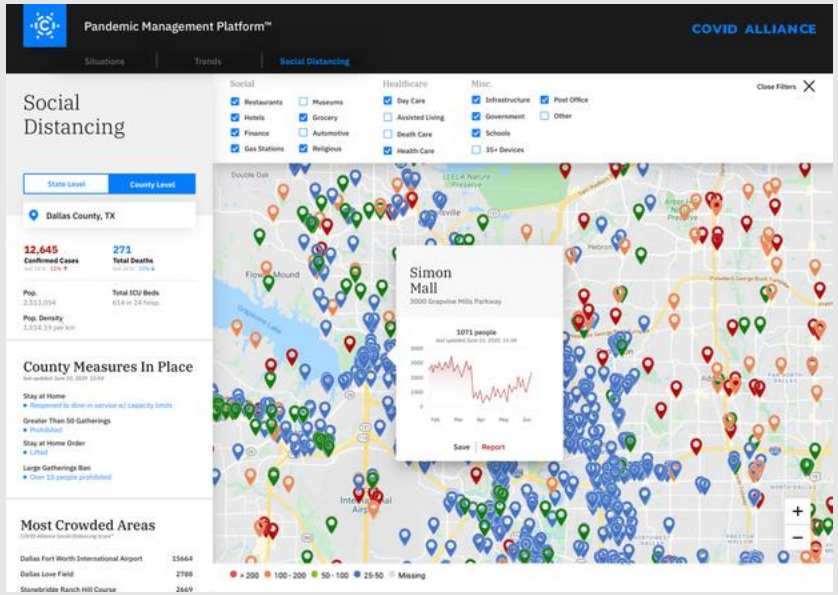
Babel Street is part of a growing ecosystem of companies taking consumer data collected by some of the world's largest corporations and mobile-app publishers, and repackaging it for intelligence, law-enforcement and military agencies.

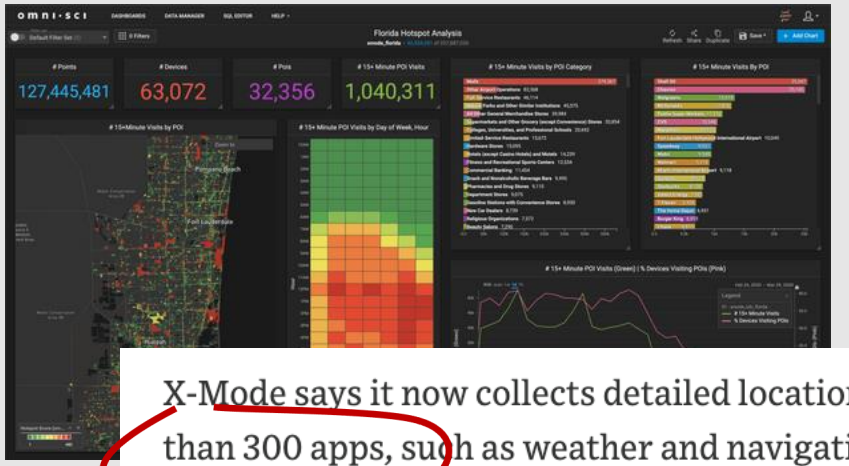
By monitoring cellphones in Russian government buildings and foreign embassies in Moscow, they were able to conclude that no high-level Russian officials or foreign diplomats had visited the test sites recently. And they homed in on the Azerbaijan trip as worthy of future study "because of contentious relations between Russia and

The sites that the Mississippi State researchers were able to pull cellphone data from were extremely sensitive: Besides drone test facilities, they also were monitoring numerous U.S. and foreign embassies and the Kremlin Senate building in Moscow, documents show.

https://www.wsj.com/articles/academic-project-used-marketing-data-to-monitor-russian-military-sites-11595073601

- Governments use cellphone location data for Covid response
  - Density of people at various places, mobility levels, etc.
  - Commercially harvested data, **not** exposure notification apps
- Also "smart" device data, eg, Kinsa thermometers to track fever





X-Mode says it now collects detailed location information from more than 300 apps, such as weather and navigation apps, many of which need users' location to function well. X-Mode pays the developers of those apps to integrate its tracking software into their designs.

https://www.wsj.com/articles/once-pariahs-location-tracking-firms-pitch-themselves-as-covid-sleuths-11592236894

- IRS attempts to use anonymized location data to find suspects

"The tool provided information as to where a phone with an anonymized identifier (created by Venntel) is located at different times," Mr. Cole said. "For example, if we know that a suspicious ATM deposit was made at a specific time and at a specific location, and we have one or more other data points for the same scheme, we can cross reference the data from each event to see if one or more devices were present at multiple transactions. This would then allow us to identify the device used by a potential suspect and attempt to follow that particular movement."

It also shows that data from the marketing industry can be used as an alternative to obtaining data from cellphone carriers, a process that requires a court order. Until 2018, prosecutors needed "reasonable grounds" to seek cell tower records from a carrier. In June 2018, the U.S. Supreme Court strengthened the requirement to show probable cause a crime has been committed before such data can be obtained

But because marketing data doesn't include names and cellphone numbers, attorneys at numerous government agencies have concluded the court decision doesn't apply.

The Journal reported in February that Department of Homeland Security agencies were buying Venntel subscriptions for immigration enforcement purposes—to detect the presence of underground border tunnels or other sites of illicit crossings. The department said at the time that the data didn't include "the individual user's identity."

Also used by DHS for immigration enforcement

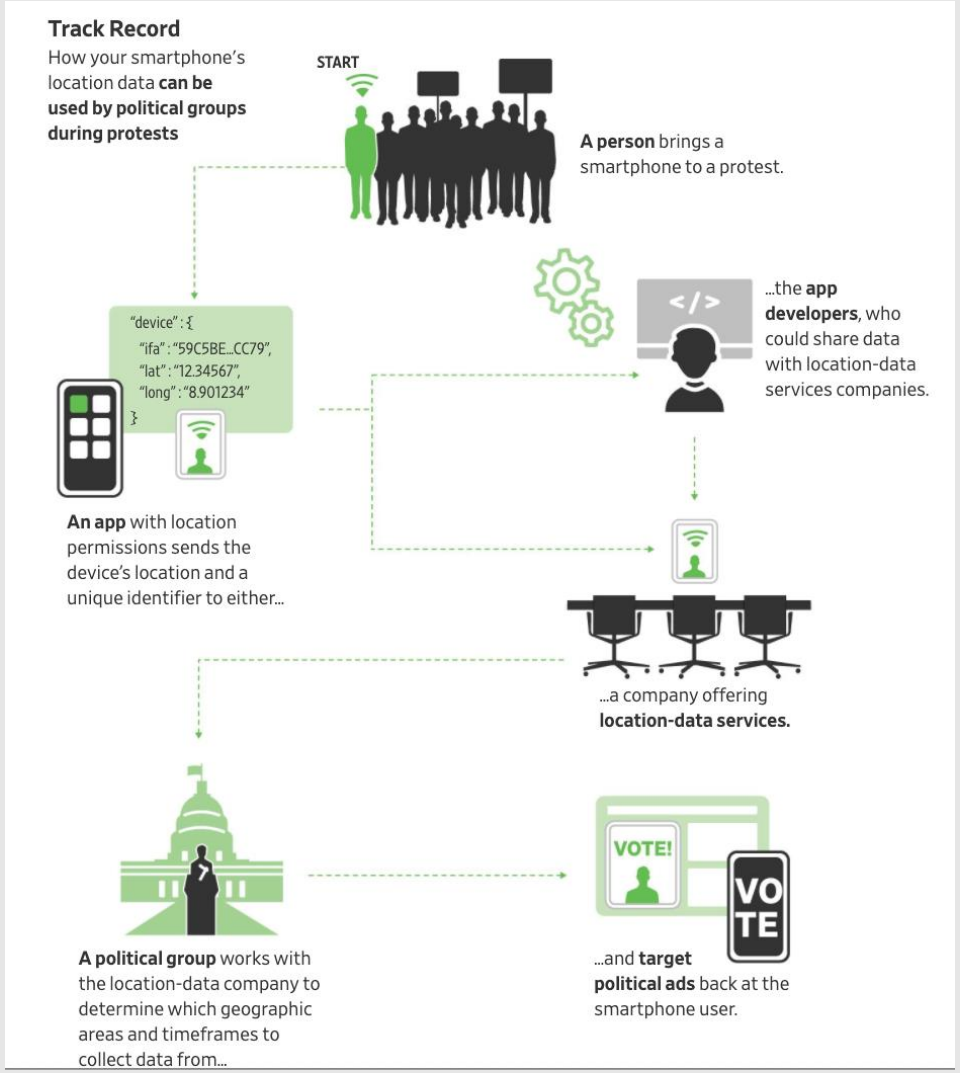
https://www.wsj.com/articles/irs-used-cellphone-location-data-to-try-to-find-suspects-11592587815

- "The data that Venntel uses is pseudonymized. Due to the confidential nature of our clients' businesses and/or missions, we are not able to comment further," Venntel President Chris Gildea said in an email."

The Journal reviewed one marketing database similar to the kind used by Venntel. In many cases, the data is precise enough to clearly identify the home address of the phone's user, which can then be cross-checked against public databases showing property ownership records or rental address history.

https://www.wsj.com/articles/irs-used-cellphone-location-data-to-try-to-find-suspects-11592587815

- Political groups use cellphone locations to identify participants in protests and rallies, target them for political advertising



https://www.wsj.com/articles/how-political-groups-are-harvesting-data-from-protesters-11592156142

A DIARY OF YOUR EVERY MOVEMENT

NYT smartphone tracking project

- Obtained a dataset of 50 billion locations from 12 million phones
  - Anonymous, but linked, so can track the same phone over time
- Source: location-tracking apps

IN MOST CASES, ascertaining a home location and an office location was enough to identify a person. Consider your daily commute: Would any other smartphone travel directly between your house and your office every day?

"Really precise, longitudinal geolocation information is absolutely impossible to anonymize. D.N.A. is probably the only thing that's harder to anonymize than precise geolocation information." -- Paul Ohm

https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html

- The inauguration weekend yielded a trove of personal stories and experiences: elite attendees at presidential ceremonies, religious observers at church services, supporters assembling across the National Mall
- Protesters were tracked just as rigorously … We spotted a senior official at the Department of Defense walking through the Women's March, beginning on the National Mall and moving past the Smithsonian National Museum of American History that afternoon. His wife was also on the mall that day, something we discovered after tracking him to his home in Virginia. Her phone was also beaming out location data, along with the phones of several neighbors… The official's data trail also led to a high school, homes of friends, a visit to Joint Base Andrews, workdays spent in the Pentagon and a ceremony at Joint Base Myer-Henderson Hall with President Barack Obama in 2017
- … rioters, too. Filtering the data to that precise time and location led us to the doorsteps of some who were there. Police were present as well, many with faces obscured by riot gear. The data led us to the homes of at least two police officers who had been at the scene.

- We lacked the mobile advertising IDs or other identifiers that advertisers often combine with demographic information like home ZIP codes, age, gender, even phone numbers and emails to create detailed audience profiles used in targeted advertising

https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html

- Risks to users

In one case, we observed a change in the regular movements of a Microsoft engineer. He made a visit one Tuesday afternoon to the main Seattle campus of a Microsoft competitor, Amazon. The following month, he started a new job at Amazon. It took minutes to identify him as Ben Broili, a manager now for Amazon Prime Air, a drone delivery service.

Watching dots move across a map sometimes revealed hints of faltering marriages, evidence of drug addiction, records of visits to psychological facilities.

Reporters hoping to evade other forms of surveillance by meeting in person with a source might want to rethink that practice. Every major newsroom covered by the data contained dozens of pings; we easily traced one Washington Post journalist through Arlington Va.

In other cases, there were detours to hotels and late-night visits to the homes of prominent people. One person, plucked from the data in Los Angeles nearly at random, was found traveling to and from roadside motels multiple times, for visits of only a few hours each time.

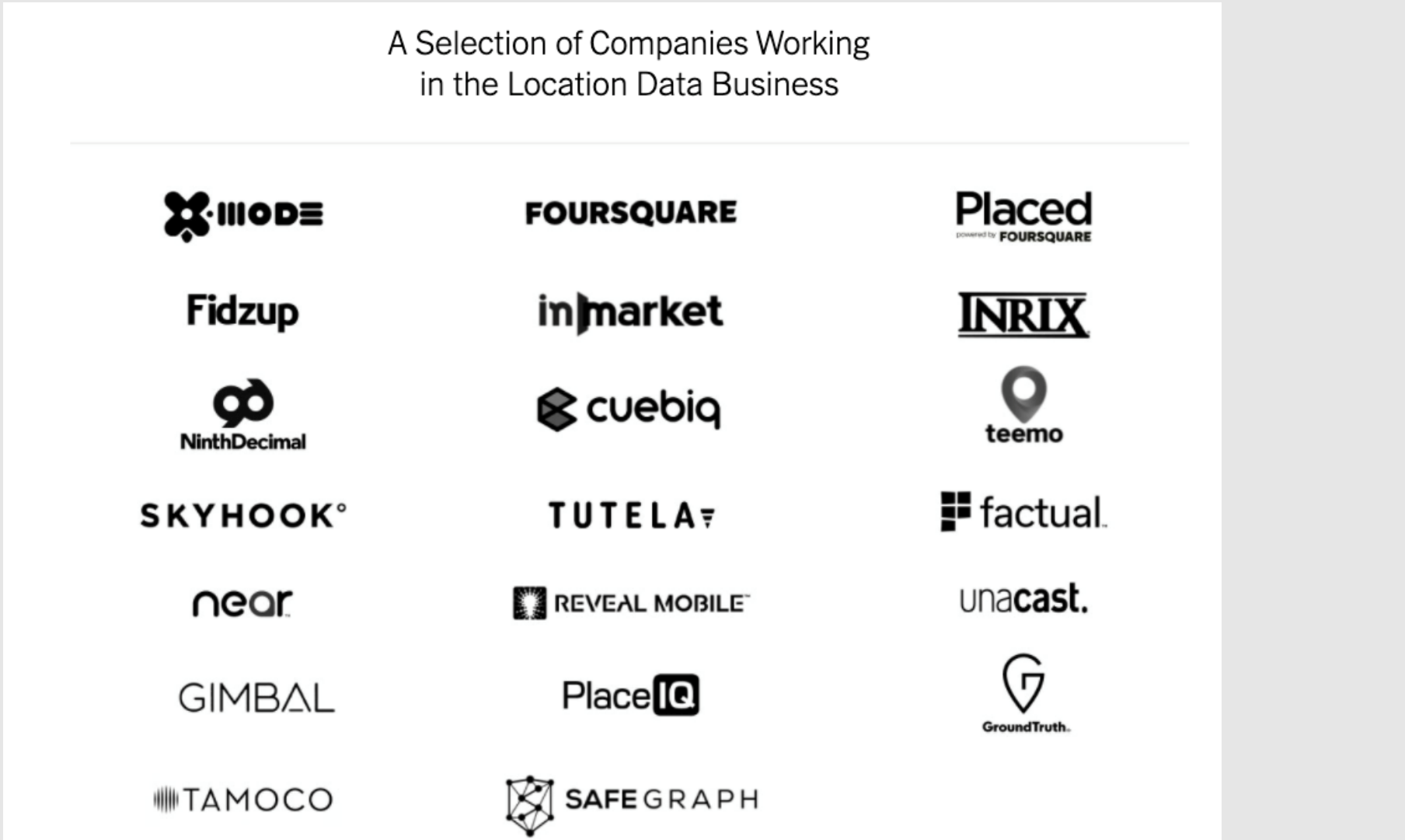
https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html

- But users know, right?

> Like many people we identified in the data, Ms. Millben said she was careful about limiting how she shared her location. Yet like many of them, she also couldn't name the app that might have collected it. Our privacy is only as secure as the least secure app on our device.

https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html

A Selection of Companies Working
in the Location Data Business



https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html