As renewed concerns over digital privacy splash across the headlines, I was recently reminded of just how much data we’re sharing with tech companies, right down to each step we take.

Specifically, while transitioning smartphones, I unlocked the depths of what Google had been collecting on me: more than 300,000 data points recording each trip to work, return home, stroll up Nicollet Mall, beer stop in Northeast, grocery run and suburban visit to my dad's.

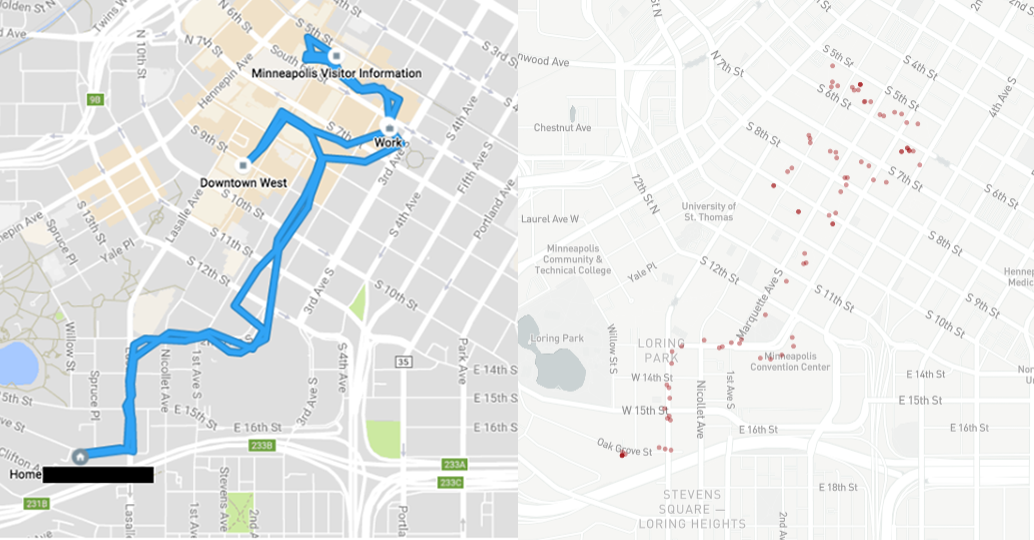
It knew the names of each business and building I walked into, without a specific check in (something I rarely do). It figured out whether I was walking, driving or riding the LRT, calculated distance and elevation and timestamped it all down to the second.

If my life could possibly be distilled down into a single dataset, this got pretty close.

I accessed this data after downloading my [Google Location History](https://www.google.com/maps/timeline?pb), a feature that's been around for awhile and is viewable one day at a time via [Google Maps Timeline](https://www.google.com/maps/timeline?pb) or via the Google Maps smartphone app. Mapping all the points spanning 2017 granted a more complete look at how much of my existence is being transmitted to Google.

Note: The process to create maps like this is a bit complex, but users can grab their full  Location History from [Google Take Out](https://takeout.google.com/settings/takeout).

For comparison, here’s what a single average weekday of my tracked locations from a couple weeks ago looks like:



“Everywhere you go can reveal so much about your life and your patterns,” said Jamie Lee Williams, a staff attorney for the Electronic Frontier Foundation. “It’s some of the most sensitive information people are giving out.”

Not everyone will be surprised by this.

Pew Research Center in 2017 [showed](http://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/) about half of Americans are skeptical of how both the government and tech companies are handling their data, and feel less secure over time. Pew also [reported](http://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/) many willingly trade their personal information away for security, useful services or popular apps.

“The price for convenience, or for cool functionality, is your privacy,” said Mike Johnson, who leads the University of Minnesota Technology Leadership Institute’s masters program in security technologies.

And my phone is full of cool and useful apps I use every day. Being directions-impaired makes me extra reliant on GPS, for example, so it’s a trade-off that Google Maps gets to know where I've been and where I'm going.

Escaping the prying eyes of satellites might not be so easy since shutting off a device's GPS disables map-based directions and cripples location-based apps. Even then, after disabling it, Johnson said wi-fi can pick up the tracking slack.

Not everyone may have this much data available on Google Maps Timeline, and will depend whether the feature was switched on, whether knowlingly or accidentally, somewhere along the line.

While [iPhones can track your location too](http://www.wired.com/2015/11/how-to-get-rid-of-the-iphone-map-that-tracks-you/), Google Location History seems to be particularly prevalent on devices using the Android operating system because Google Maps automatically comes with it, and it's easy to just agree to turn it on. Android-powered devices represent around 80 percent of the global smartphones, and about half in the U.S.

Some may find this feature cool and useful. Others might be uncomfortable with third parties knowing so much about their daily activities. So Google Location History data can be [disabled or deleted](https://support.google.com/accounts/answer/3118687?hl=en), and the instructions may differ between devices. Note too that other apps might be doing something similar.

Location data, of course, represents a tiny fraction of the information Google and other tech companies collect about people. Facebook, for instance, was just revealed to be collecting the texts and phone calls of some users.

“People can’t really comprehend what they’re giving to these companies,” Williams said.

Users do have some control over what they share though, Johnson said, so it’s a good idea to audit what apps are collecting what. People can also download and review their own data from Facebook, Google, Twitter and elsewhere.

“You’re not going to leave your physical possessions unprotected,” he added, and that users need to "take a breath" and take stock of what digital information they could be exposing to the wider world.

“The most important asset you have is your privacy and your identity,” he said.