Electronic eyes are watching us everywhere, tracking our purchases, conversations and even each step we take.

My smartphone, for instance, knows each location I've visited. Many people's devices are do the same and send that data to Google and other tech companies.

How well those companies protect digital privacy is under constant scrutiny, as recent headlines about Facebook's Cambridge Analytica woes attest.

Vast amounts of data are generated daily -- of which my phone's contents represent a tiny fraction --  and gathered by both seen and unseen actors at an increasing pace sometimes to detrimental effect, like last year’s Equifax cybersecurity breach affecting millions of consumers.

Not that many users expected much more. 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 are feeling less secure over time. Pew also [reported](http://www.pewinternet.org/2016/01/14/privacy-and-information-sharing/) many are willing to trade their personal information away anyway 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.

But seeing what data we’re sharing in its entirety might lend a different perspective. When I mapped my location data, for instance, even I was surprised by its extent.

<strib type="text" data="<style type='text/css'>.dataframe{height:400px;} @media only screen and (min-width: 200px) and (max-width: 767px){.dataframe {height:400px;}}</style><div class='embed'><iframe class='dataframe' src='http://datadrop-dev.startribune.com/20180329-gps\_tracking/build' border='0' frameborder='0' scrolling='no' width='100%' height='400'></iframe></div>"></strib>

That’s a map representing nearly everywhere I went in Downtown Minneapolis for roughly a year – just sampling more than 300,000 data points, represented by tiny red dots scattered across the city, state and country -- meticulously tracked over the lifetime of two different Android-based smartphones.

And the data is extremely detailed.

Google Location History tracks a user’s location, whether they’re walking, riding or driving, calculates distance and elevation, figures out which businesses and buildings they’ve visited without a specific check-in and much more, all time-stamped. The feature has been around awhile, and those being tracked like this likely switched it on at some point, maybe without even realizing it.

“Data that once seemed innocuous or benign before can really impact a person,” Johnson said.

A user's data is viewable via [Google Maps Timeline](https://www.google.com/maps/timeline?pb), which shows a day's worth of activity at a time. Displaying all the data at once is slightly more involved. Using some digital magic, I converted the data and mapped all the points from 2017, granting a more complete look at how much of my life is being transmitted to Google.

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

<img src=”http://datadrop-dev.startribune.com/20180329-gps\_tracking/build/img/compare.png” width=”100%”  />

“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.”

And not giving it out can be more difficult than it seems. Shutting off your device's GPS disables map-based directions and cripples location-based apps. And even if you do shut it off, Johnson said wi-fi can pick up the tracking slack.

Not everyone may have this much data available on Google Maps Timeline. It will depend upon how a device is configured and if the tracking feature is enabled. It seems to be particularly prevalent on devices using the Android operating system, which in 2017 represented more than 80 percent global market share among smartphones (though location tracking [works on iPhones too](https://www.wired.com/2015/11/how-to-get-rid-of-the-iphone-map-that-tracks-you/)).

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 [can be disabled or deleted](https://support.google.com/accounts/answer/3118687?hl=en), and the method for doing so depends upon the device.

Remember too that disabling Google Location History doesn't mean other apps aren't also tracking you.

Location data, of course, represents a tiny fraction of the information Google and other tech companies collects about people, which also includes the emails, texts, search history, app usage, phone calls, social networks and myriad other bits of data being rounded up and analyzed to fuel algorithms and better understand user habits, wants and needs.

“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. Users 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.