Introduction

Joe:

It’s a black and white aerial photograph. The building is immediately recognizable: the Pentagon. As you scroll down the page, the picture is covered with hundreds of tiny green dots: in the parking lot, on the roads, in the parks but also in the Pentagon itself, one of the most secure buildings in the world. Each of these dots represents a cell phone, in someone’s pocket or hand, on their desk or dashboard. It’s an exact photograph of where hundreds of people were located on a specific day in 2016.

Same bird’s eye view, same green dots, this time on a beach in L.A., or on a block on Wall Street, in Beverly Hills or Central Park.

Journalists at The New York Times managed to access a total of 50 billion location pings, from 12 million cell phones. It’s the first time the press has worked with such an enormous data set. They collected this data from an anonymous source who urgently wanted to inform the public: the devices we carry with us everywhere, all day, our phones are constantly sending location data to companies specialized in tracking us.

Hello Chloe!

Chloe:

Hi there Joe!

Joe:

Welcome to the Memo, the podcast that breaks down the latest big issues in the digital world. Today we’ll be talking about how secure your personal data really is. Chloe, the New York Times report I just mentioned is chilling…but before getting into it, let’s look at what exactly we’re talking about. How does geolocation work?

Chloe:

What I find really interesting is that you can locate phones even when their GPS function—the global positioning system that works by satellite—is deactivated. That’s according to the business technology website ZDNet, reporting on research conducted by Northeastern University in Boston.

So how come? Our phones are equipped with sensors: an accelerometer, a magnetometer, which is used as a kind of compass, and a gyroscope, which measures orientation. This information is then crossed with wireless networks and cellular data. So if your phone is connected to wireless, it’s very easy to know its location.
What’s the point of all these sensors?

— Chloe:

Well, first and foremost, they’re useful to us and we use them to connect to wireless networks. But apps that help locate you on a map and plan out your itinerary are also using this geolocation data. In fact, on a smartphone, a great number of apps are using this data. Your weather app, for instance, and maybe your internet browser to help you navigate better. They also might remember your personal data. One article I read in *Bien vivre le digital* reminds us that we can check our settings to see which apps have been granted access to our phone’s GPS. You’d be surprised by how many...

— Joe:

And some people jumped right into developing tattle-tale apps that rely on this data...

— Chloe:

That’s right: we’re talking about the apps made for parents to track their children. All you need is an invisible tracker in the child’s phone, an app on the adult’s phone, and the parent can relax.

But *Le Figaro* reports that these apps are sometimes used for other, more disturbing purposes, by abusive spouses for instance. Here I quote: “In 2018, the Hubertine-Auclert Center for gender equality published a report on cyberviolence. 21% of 302 victims claimed they had been monitored through spy software or other tracking devices.” And that’s just the people who noticed they were being spied on; it’s very hard to detect. These practices are a punishable offence, can lead to a fine of up to 45,000 Euros...and a new bill is in the works to strengthen these penalties.

— Joe:

That’s reassuring news! It’s easy to imagine how these trackers could be used much more widely for mass surveillance...

— Chloe:

Exactly. That’s what’s happening in China in the Xinjiang (SHIN-JAN) region. Everyone, including journalists and tourists, have to hand over their phones when crossing the border. The Guardian, in partnership with other media, investigated the situation and found that the authorities had implemented this measure to install a hidden app that would search the phone for forbidden documents and probably also track the phone’s location.

— Joe:

But collecting geolocation data can also be perfectly legal...

— Chloe:

Yes, that’s exactly what the New York Times investigated, in the report you mentioned earlier. The journalists listed several companies that have made it their bread and butter. You probably won’t recognize their names, but at least one of them has most likely used your phone. These companies collect your geolocation data to sell them to advertisers who then serve you targeted ads. Two of these companies are French: Teemo and Fidzup. And what they do is perfectly legal. They ask apps, like your weather app for instance, to install...
a small piece of code that will store your location, in exchange for advertising revenue. They then sell this data to their clients...who value this information very much, because by knowing that you've been in their store for instance, they can send you tailored ads.

— Joe:

And that’s legal.

— Chloe:
Yes, completely legal, because the files have been made anonymous. The tracking company doesn’t send their clients an Excel sheet with your name, phone number and location. The location data is linked to an advertising number, attributed to your phone (a number that you can in fact change in your own settings to wipe the slate clean).

— Joe:
So anonymizing data is what makes geolocation legal. As long as my data can’t be traced back to me, it’s alright.

— Chloe:

Right. But truth is, when you start linking up the data points, you can piece together entire itineraries. And these itineraries are unique: my home, my workplace, my usual hangouts...reporters at the New York Times were able to reestablish the itineraries of someone like an engineer at Microsoft, who one day went to Amazon’s offices...and then several weeks later, changed jobs. The engineer in question confirmed all this. They also followed the paths of investigative journalists, military officials, and policemen as they went home from work...so the data isn’t all that anonymous, and in case of a cyberattack, could fall into the wrong hands.

— Joe:
But how do you get from a series of linked data points to an individual?

— Chloe:
In 2013, researchers ran a study on this, which they published in the scientific journal Nature. They gathered data from a million and a half users over a period of 15 months...and discovered that the tracks we leave behind is unique, more unique in fact than our own fingerprints. For your fingers, you need 12 data points to identify who you are; whereas for geolocation, they only needed 4 data points to identify 95% of the people they were tracking.

— Joe:
Within the EU, does GDPR protect us from any of these practices?

— Marine:
Well, it makes things more transparent. The General Data Protection Regulation requires companies to inform users whenever they collect data for targeted advertising, and this includes geolocation. Several companies, including Fidzup and Teemo, were warned for poorly implementing this. But as an article in Numerama reminds us, collecting and sharing location data remains legal--as long as users are in the know and can ask for their data to be erased.

— Joe:
Do we have any advice for our listeners? What can they do to protect their data?

— Chloe:
Yes, the CNIL, the French supervisory authority, has a lot of great advice, you’ll find a link to their page in the description of this episode. Among their tips: deny access to your location for apps that don’t need it (you’d be surprised: when I did this, it turned out the app I use to record sound had access to my location). Then, regularly renew your mobile ad ID, to cut the string of geolocation data associated with it.

And remember, technology isn’t foolproof either: 32 prisoners in Denmark were freed in late 2019. Why? Because they were wrongly suspected based on flawed geolocation data. You can read all about it in the Guardian.

— Joe:
Thank you Chloe, and thank you to our listeners. This episode is the first in our mini-series on personal data. Next up, we’ll be talking about whether our devices are listening in on our conversations. In the meantime, you can find all the links to the sources we used below, and we’ve even added a few extra ones if you want to dig deeper. Until next time, goodbye!

Resources:
Bien vivre le digital: https://bienvivreledigital.orange.fr/mes-donnees-mon-identite/gerer-ses-donnees-personnelles/la-geolocalisation-sur-mobile
The Guardian: https://www.theguardian.com/world/2019/jul/02/chinese-border-guards-surveillance-app-tourists-phones
Nature: https://www.nature.com/articles/srep01376
CNIL: https://www.cnil.fr/fr/maitrisez-les-reglages-vie-privee-de-votre-smartphone

To dig deeper:
https://apnews.com/828aefab64d4411bac257a07c1af0ecb
https://techcrunch.com/2017/08/22/accuweather-revealmobile-ios/