Michael Kwet, “In Stores, Secret Surveillance Tracks Your Every Move”
Imagine you are shopping in your favorite grocery store. As you approach the dairy aisle, you are sent a push notification in your phone: “10 percent off your favorite yogurt! Click here to redeem your coupon.” You considered buying yogurt on your last trip to the store, but you decided against it. How did your phone know?
Your smartphone was tracking you. The grocery store got your location data and paid a shadowy group of marketers to use that information to target you with ads. Recent reports have noted how companies use data gathered from cell towers, ambient Wi-Fi, and GPS. But the location data industry has a much more precise, and unobtrusive, tool: Bluetooth beacons.
These beacons are small, inobtrusive electronic devices that are hidden throughout the grocery store; an app on your phone that communicates with them informed the company not only that you had entered the building, but that you had lingered for two minutes in front of the low-fat Chobanis.

How Accurate Are Bluetooth Beacons?
Most location services use cell towers and GPS, but these technologies have limitations. Cell towers have wide coverage, but low location accuracy: An advertiser can think you are in Walgreens, but you’re actually in McDonald’s next door. GPS, by contrast, can be accurate to a radius of around five meters (16 feet), but it does not work well indoors.
Bluetooth beacons, however, can track your location accurately from a range of inches to about 50 meters. They use little energy, and they work well indoors. That has made them popular among companies that want precise tracking inside a store.
Most people aren’t aware they are being watched with beacons, but the “beacosystem” tracks millions of people every day. Beacons are placed at airports, malls, subways, buses, taxis, sporting arenas, gyms, hotels, hospitals, music festivals, cinemas and museums, and even on billboards.
In order to track you or trigger an action like a coupon or message to your phone, companies need you to install an app on your phone that will recognize the beacon in the store. Retailers (like Target and Walmart) that use Bluetooth beacons typically build tracking into their own apps. But retailers want to make sure most of their customers can be tracked — not just the ones that download their own particular app.
So a hidden industry of third-party location-marketing firms has proliferated in response. These companies take their beacon tracking code and bundle it into a toolkit developers can use.
The makers of many popular apps, such as those for news or weather updates, insert these toolkits into their apps. They might be paid by the beacon companies or receive other benefits, like detailed reports on their users.
Location data companies often collect additional data provided by apps. A location company called Pulsate, for example, encourages app developers to pass them customer email addresses and names.
Companies like Reveal Mobile collect data from software development kits inside

hundreds of frequently used apps. In the United States, another company, inMarket, covers 38 percent of millennial moms and about one-quarter of all smartphones, and tracks 50 million people each month. Other players have similar reach.

Location data companies have other disturbing tricks up their sleeve. For example, inMarket developed "mindset targeting" techniques that predict when individuals are most receptive to ads. These techniques are based on statistical probabilities calculated through millions of observations of human behavior. Brands like Hellman's, Heineken and Hillshire Farms have used these technologies to drive product campaigns.

What is an S.D.K.?

A Software Development Kit is code that's inserted into an app and enables certain features, like activating your phone's Bluetooth sensor. Location data companies create S.D.K.s and developers insert them into their apps, creating a conduit for recording and storing your movement data.

Location marketing aims to understand "online-offline attribution." If a Starbucks coffee ad is sent to your email, for example, marketers want to know if you actually went there and bought a coffee. The only way to know is to monitor your online and offline habits at all times.

Beacons are also being used for smart cities initiatives. The location company Gimbal provided beacons for LinkNYC kiosks that provoked privacy concerns about tracking passers-by. Beacon initiatives have been started in other cities, including Amsterdam (in partnership with Google), London and Norwich.

Familiar tech giants are also players in the beacosystem. In 2015, Facebook began shipping free Facebook Bluetooth beacons to businesses for location marketing inside the Facebook app. Leaked documents show that Facebook worried that users would "freak out" and spread "negative memes" about the program. The company recently removed the Facebook Bluetooth beacons section from their website.

Not to be left out, in 2017, Google introduced Project Beacon and began sending beacons to businesses for use with Google Ads services. Google uses the beacons to send the businesses' visitors notifications that ask them to leave photos and reviews, among other features. And last year, investigators at Quartz found that Google Android can track you using Bluetooth beacons even when you turn Bluetooth off in your phone.

For years, Apple and Google have allowed companies to bury surveillance features inside the apps offered in their app stores. And both companies conduct their own beacon surveillance through iOS and Android.

It should not be lost on the public that Apple created the first Bluetooth system of commercial surveillance. Apple's chief executive, Tim Cook, recently wagged his finger at the "data-industrial complex." Unlike other tech giants that monetize surveillance, Apple relies upon hardware sales, he said. But Mr. Cook knew what Apple was creating with iBeacon in 2013. Apple's own website explains to developers how they can use iBeacon to micro-target consumers in stores.

Companies collecting micro-location data defend the practice by arguing that

users can opt out of location services. They maintain that consumers embrace targeted ads because they're more relevant. Industry players further claim that data is anonymized through techniques that mask the identification of users. Your data may be stored as "ID-67aGb9ac72r" instead of "Jane Doe." Yet studies have shown that it is relatively easy to deanonymize mobility data. Moreover, the process of "informed consent" fails to protect user privacy. As The Times noted in an investigation into smartphone location tracking, "The explanations people see when prompted to give permission are often incomplete or misleading."

For informed consent using beacons, you have to first know that the beacons exist. Then, you have to know which places use them, but venues and stores don't put up signs or inform their customers. You can download an app like Beacon Scanner and scan for beacons when you enter a store. But even if you detect the beacons, you don't know who is collecting the data. Let's say you visit Target; it might be collecting data from you, but it might rent its beacons out to other businesses, allowing them to monitor your location. Moreover, some beacons are not secured, so third parties can "piggyback" off public beacons and use them to collect your location. There is no way to know if a store has secured its beacons.

Apple and Google could be tracking you through iOS and Android, but they don't make their Bluetooth beacon collection methods transparent. There is no easy way to determine which apps on your phone have the beacon location tracking built in.

Even if you did know which companies have access to your beacon data, there's no way to know what kind of data is collected through the app. It could be your micro-location, dwell time or foot traffic, but it can also include data from the app, such as your name, and your app data can be combined with other data sets compiled about you by data brokers. There is simply no transparency.

To protect yourself from beacons in the short term, you can delete any apps that may be spying on you — including apps from retailers — and shut off location services and Bluetooth where they are not needed. You can also follow The Times's guide on how to stop apps from tracking your location. For Android users, the F-Droid app store hosts free and open- source apps that do not spy on users with hidden trackers.

Most of our concerns about privacy are tied to the online world, and can feel theoretical at times. But there is nothing theoretical about Bluetooth beacon technology that follows you into retail stores (and other venues) and tracks your movement down to the meter.

Michael Kwet is a visiting fellow at the Information Society Project at Yale Law School, and host of the Tech Empire podcast.