افغانستان آزاد ــ آزاد افغانستان

AA-AA

چو کشور نباشد تن من مبـــــاد بدین بوم و بر زنده یک تن مــــباد
همه سر به سر تن به کشتن دهیم از آن به که کشور به دشمن دهیم

www.afgazad.com afgazad@gmail.com

European Languages	زبانهای اروپائی

SEPTEMBER 6, 2018

by MICHAEL KWET
07.09.2018

Google and Apple's Systems to Track you in Person: What the Media Isn't Telling You

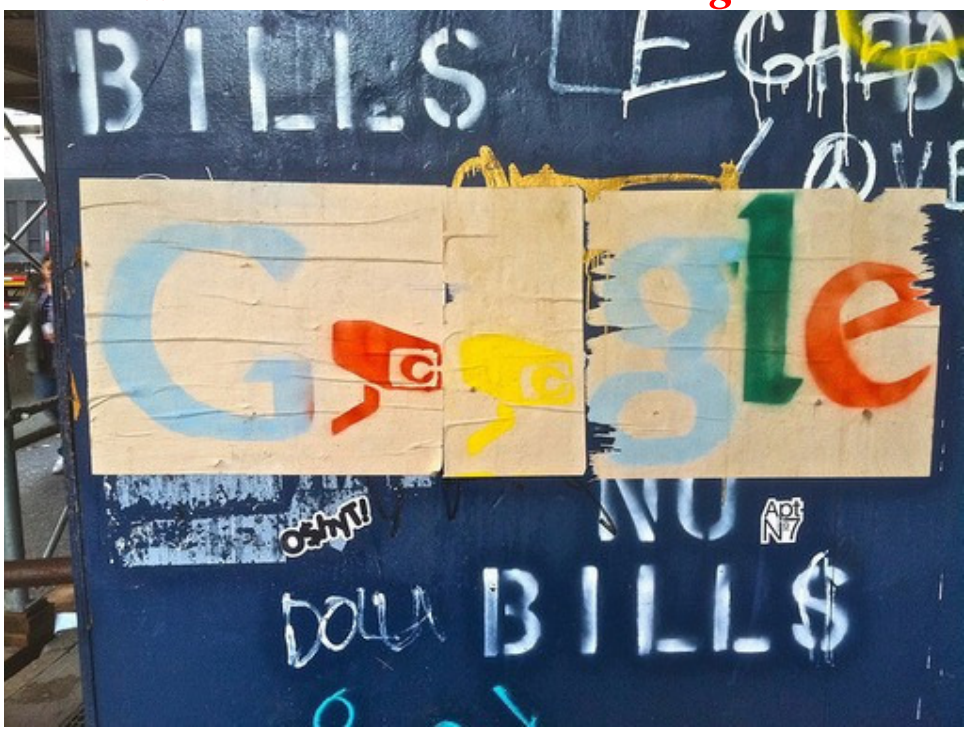

Photo Source Tyler Merbler | CC BY 2.0

Google is in the news (again) for creepy surveillance practices. Google, AP reported, is tracking your physical whereabouts even after you tell them to shut Location History off. Now Bloomberg reports they bought data about Mastercard transactions to link online ads with in-store purchases. These make for interesting stories, but the real story, not being discussed, is the online-physical advertising systems engineered by Google and Apple.

Over the last few years, there's been a quiet revolution in retail marketing empowering advertisers to track consumers in physical space. Retailers have realized that, contrary to popular misconceptions, most retail purchases are still made in brick-and-mortar stores– not the online world of Amazon and Walmart. The capacity to track each of us in the physical world offers an untapped market for high-tech advertising. Google previously called this the Physical Web, a new Internet of Things frontier that melds the online and offline worlds into one.

To facilitate online-offline tracking, Google and Apple developed protocols for communications with mobile devices like smartphones. The idea is to make the physical world, like a poster on a building, something you can "click on" (i.e. interact with) without installing a special app. The dominant weapon of choice is the bluetooth beacon – silly putty-sized units that broadcast bluetooth signals to track your precise location and send messages to your phone. Bluetooth beacons are now scattered about stores, airports, sporting arenas, malls, and other locales. The technology is several years in the making.

Back in 2013, Apple launched its iBeacon to much fanfare within the ad industry. Target, Rite Aid, Walmart, and American Eagle were among the first adopters. Not to be outdone, Google announced UriBeacon in 2014, which evolved into the Eddystone protocol.

In parallel, Google developed its Nearby APIs for incorporation into your phone. Google software scans the area around your device for bluetooth beacons (including iBeacons), which can then track you and broadcast messages to your phone. For example, if you walk by a bluetooth beacon, it might push a website URL to your phone that will display in your Nearby Notifications.

Bluetooth beacons function as a "light house" to broadcast signals to mobile devices like smartphones and tablets. Unlike GPS, which can misread your location by a matter of several meters, bluetooth can determine your location with fine precision. If you walk down an aisle and a beacon is nearby, the beacon owner (retailers, advertisers, or product vendors) can determine you're in that particular aisle or department. Beacon signals can reach up 70 meters.

Added to this, individual apps often package in "tracker SDKs" that collect various forms of smartphone data and activity. A team of researchers found that over 7 in 10 apps incorporate hidden trackers (usually to monetize surveillance). Some of these trackers surveil your physical location using GPS, bluetooth, WiFi, or near-ultrasonic sound.

Physical location tracking is highly coveted by Big Data analysts, who are eager to exploit the coming IoT surveillance society. Marketers aim to serve you "interactive" shopping

experiences while tracking you across the "marketing funnel". If you view a KFC advertisement at home, for example, how can they know you went to the store to buy the latest chicken sandwich? If you're in a store, why not guide your shopping with an app, while "nudging" you with targeted ads?

"Proximity marketing", as it's known in the industry, aims to transform physical shopping into a total surveillance experience, bringing us one step closer to a Minority Report world. Will this become the new normal?

According to industry reports, the proximity tracking industry is expanding at a steady pace. Proximity location company Unacast says that 75% of the top twenty US retailers have implemented beacons. In 2015, Unacast's Proximity Directory included almost 900,000 proximity sensors across the world. By 2017, they registered 18.7million– a twenty-fold increase in just two years. The beacon market is expected to surpass $25 billion by 2024.

All of this is made possible by the two major "innovators" of the mobile space – Apple and Google – as well as a complementary ecosystem of tracker companies hidden from public view. Large industry players like Salesforce offer integration with beacons, while smaller companies like Estimote, Swirl, and Mobiquity provide their own solutions. Industry giants like Microsoft, Adobe, and Facebook are also digging into the technology.

Some uses are disturbing, but not surprising. Retailers monitor your "dwell time" – how long you stay in one spot in the store. Companies like Safegraph can offer "foot traffic analysis" to help the financial industry and brick-and-mortar franchises pick new store locations. Others use geofencing to nudge the herd: when you enter a geofenced zone like Starbucks, they can push ads or coupons to your phone. Alternatively, as you enter Starbucks, a rival like Dunkin Donuts can send you a message to come their way instead.

The Big Data collected by proximity companies is merged into larger data sets and analyzed by corporations like Salesforce, whose "intelligent marketing hub" uses advanced statistics and AI to "stitch together" user identities across devices (laptop, smartphone, tablet), segment each of us into categories (like gender, age, and location), and drive us along personalized advertising campaigns.

Most people have no clue that Google and Apple have them interacting with this corporate netherworld. The whole economy is made possible by the legal fiction of "informed consent". Google's response to this round of criticism is, effectively, "consumers can opt out". Yet nobody truly chooses to opt in.

There are deeper lessons here. Behind the scenes, the strategy of surveillance capitalism is to continue building an enormous ecosystem backed by rich investors and heavy hitters across industries – chip fabs, cloud server farms, specialized hardware, and many thousands of companies to provide data services. Taken together, they are too big to fail. Providing genuine, simple privacy now means incinerating the Big Data surveillance industry.

Any arising controversy will be sucked into never-ending court battles over minor tweaks that produce slightly higher degrees of transparency or slightly greater limitations on how our data is used. Europe provides a good example: now that the GDPR has passed, everyone is still under surveillance.

Apple claims to be better than Google – they are a "hardware company", not data miners, they insist. Yet iBeacons provide just one example of many to the contrary. The real root of the problem is state-corporate control of the digital ecosystem– software systems and digital infrastructure.

Can we stop the emerging Internet of Stings, and with it, surveillance capitalism? To secure real privacy, it's going to take a movement more committed than the battle for net neutrality. We need to take close look at the players linked to the advertising industry – and their vision for the future – to get a sense of what we're up against.

Michael Kwet is a Visiting Fellow of the Information Society Project at Yale Law School. His podcast, Tech Empire, can be accessed in iTunes and on SoundCloud. He is currently writing a book, "Tech Empire: Digital Colonialism in the Global South".