As Your Phone And TV Track You, Political Campaigns Listen In

Who isn't tracking you these days? Technocrats thrive on data, without which their precious AI programs will sit there like inert rocks. National privacy legislation is desperately needed. TN Editor

It was a crowded primary field and Tony Evers, running for governor, was eager to win the support of officials gathered at a Wisconsin state Democratic party meeting, so the candidate did all the usual things: he read the room, he shook hands, he networked.

The digital fence enabled Evers' team to push ads onto the iPhones and Androids of all those attending the meeting. Not only that, but because the technology pulled the unique identification numbers off the phones, a data broker could use the digital signatures to follow the devices home. Once there, the campaign could use so-called cross-device tracking technology to find associated laptops, desktops and other

devices to push even more ads.

Welcome to the new frontier of campaign tech — a loosely regulated world in which simply downloading a weather app or game, connecting to Wi-Fi at a coffee shop or powering up a home router can allow a data broker to monitor your movements with ease, then compile the location information and sell it to a political candidate who can use it to surround you with messages.

“We can put a pin on a building, and if you are in that building, we are going to get you,” said Democratic strategist Dane Strother, who advised Evers. And they can get you even if you aren’t in the building anymore, but were simply there at some point in the last six months.

Campaigns don’t match the names of voters with the personal information they scoop up — although that could be possible in many cases. Instead, they use the information to micro-target ads to appear on phones and other devices based on individual profiles that show where a voter goes, whether a gun range, a Whole Foods or a town hall debate over Medicare.

The spots would show up in all the digital places a person normally sees ads — whether on Facebook or an internet browser such as Chrome.

As a result, if you have been to a political rally, a town hall, or just fit a demographic a campaign is after, chances are good your movements are being tracked with unnerving accuracy by data vendors on the payroll of campaigns. The information gathering can quickly invade even the most private of moments.

Antiabortion groups, for example, used the technology to track women who entered waiting rooms of abortion clinics in more than a half dozen cities. RealOptions, a California-based network of so-called pregnancy crisis centers, along with a partner organization, had hired a firm to track cell phones in and around clinic lobbies and push ads touting alternatives to abortion. Even after the women left the clinics, the ads continued for a month.

That effort ended in 2017 under pressure from Massachusetts

authorities, who warned it violated the state's consumer protection laws. But such crackdowns are rare.

Data brokers and their political clients operate in an environment in which technology moves much faster than Congress or state legislatures, which are under pressure from Silicon Valley not to strengthen privacy laws. The RealOptions case turned out to be a harbinger for a new generation of political campaigning built around tracking and monitoring even the most private moments of people's lives.

Read full story here…