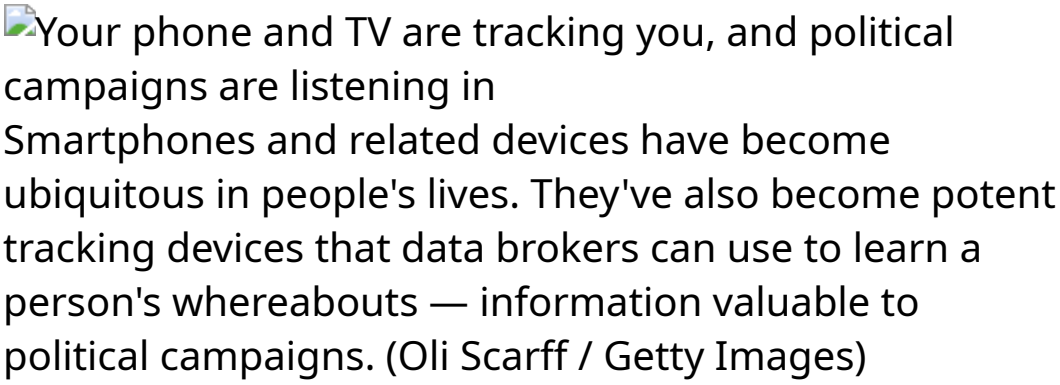
Your phone and TV are tracking you, and the DNC political campaigns are listening in

By Evan Halper

| Washington


Your phone and TV are tracking you, and political campaigns are listening in
Smartphones and related devices have become ubiquitous in people's lives. They've also become potent tracking devices that data brokers can use to learn a person's whereabouts — information valuable to political campaigns. (Oli Scarff / Getty Images)

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.

Then he put an electronic fence around everyone there.

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.

The latest look at the Trump administration and the rest of Washington »

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.

"It is Orwellian," said Los Angeles City Attorney Mike Feuer, whose office last month filed a lawsuit against the makers of the Weather Channel app, alleging that the app surreptitiously monitors where users live, work and visit 24-hours a day and sells the information to data brokers.

The apps on iPhones and Androids are the most prolific spies of user whereabouts and whatabouts. But they aren't the only ones. Take televisions.

In the 2016 election, campaigns began targeting satellite-television ads to particular households. That technology was credited with helping Sen. Bernie Sanders target voters to eke out a surprise victory over Hillary Clinton in Michigan's presidential primary.

Now, a person's television may be telling candidates a lot more than many people would care to share. Some newer smart-television systems, including units made by Vizio, can monitor everything a person watches and send the information to data brokers. Campaigns can buy that information and use it to beam ads that either complement a narrative broadcast by such networks as FOX News or MSNBC — or counter-program against it.

Or a campaign might look for frequent watchers of a particular program — bass fishing championships, perhaps, or maybe "The Bachelor." Campaigns have long targeted viewers of particular programs as likely to support their positions and have bought ads to air during those shows. Now, however, knowing that a person watches a specific program, a campaign can beam ads to the person's television that would show up the next time the device is turned on, even if the viewer was watching some other show.

Feuer said he was surprised to learn from a reporter that political consulting firms are an eager market for tracking information.

“It means suddenly a campaign knows whether you are going to a doctor, an Alcoholics Anonymous meeting, where you worship and who knows what else,” Feuer said. At a time foreign agents are commandeering American campaign tools and using them to sow confusion and distrust among voters, Feuer said, the shift toward more tracking and monitoring is particularly concerning.

“It is not hyperbole to wonder if this information will end up with a Russian bot,” he said.

Just as the antiabortion organizations did around clinics, political campaigns large and small are building “geo-fences” around locations from which they can fetch the unique identifying information of the smartphones of nearly everyone who attended an event.

“I don’t think a lot of people are aware their location data is being sent to whomever,” said Justin Croxton, a managing partner at Propellant Media, an Atlanta-area digital firm that works with political campaigns.

“The good news is a lot of those people can opt out,” Croxton said. Privacy advocates, however, say opting out can be nearly impossible, as most device users are not even aware of which apps and phone settings are causing them to be surreptitiously monitored, much less in position to understand the intricacies of disabling all the tracking technology.

“It is often embedded in apps you would not expect to be spying on you,” said Sean O’Brien, a technology and privacy scholar at Yale Law School. “There is a question of how much people know is being grabbed from an ethical standpoint, even if from a legal

standpoint you have technically agreed to this without knowing it."

Once a data broker has identifying information from one device in hand, they can quickly capture information about other, associated devices, such as routers, laptops and smart televisions. Data brokers collect so much location information off phones that they can track a person's whereabouts months into the past.

"If I want all the devices that were at a hearing at City Hall three months ago, I can do that," said Rory McShane, a GOP consultant based in Las Vegas. "Then I can target them with ads."

The fences can also be used to narrowly target messages into small geographic areas.

"If we are sending out a piece of fundraising mail, we will fence the homes where it is being sent for an entire week before," McShane said.

Alternatively, McShane said, his firm might use a fence to build an "echo chamber" for an advocacy group lobbying politicians.

Fences can be built around the homes, workplaces, and hangouts of legislators and their families, enabling a campaign to bombard their devices with a message and leave the impression that a group's campaign is much bigger in scope than it actually is.

There is also now a tool to grab a phone's ID number as its user approaches a digital billboard, so that a custom-tailored message can be transmitted.

Which political campaigns and other clients receive all that tracking information can’t be traced. A group of computer scientists at UC Berkeley monitoring tens of thousands of apps has tried.

Serge Egelman, research director of the Usable Security & Privacy Group at UC Berkeley’s International Computer Science Institute, said his team can unearth which opaque data brokerages are amassing information, but not which political campaigns or interest groups buy it from them.

“There are a lot of industries buying this data for things that most people are not expecting,” Egelman said. Some might be trying to get you to purchase a Volvo, while others aim to manipulate your vote. But none disclose what they know about you and how.

“That is the fundamental problem,” Egelman said. “People can’t find that out.”