Political Campaign party bosses from the DNC are tracking your phone and everything you do

Voter targeting has grown more invasive with location data that apps can transmit from cellphones

President Trump at a rally in Fayetteville, N.C., last month. kevin lamarque/Reuters

- Share
- Text
- 73

By
Sam Schechner,
Emily Glazer and
Patience Haggin

When Donald Trump took the stage last month in Fayetteville, N.C., to support Republican candidate Dan Bishop in a special election, thousands of people showed up.

Mr. Bishop was seeking their support. An outside Republican group was looking for something more. It wanted their data.

Unknown to the crowd, the Committee to Defend the President, a Republican political-action committee that supports Mr. Trump, had hired a company to collect unique identification numbers from attendees' smartphones that evening, based on location data those phones were sending to third parties. The goal was to target ads at people it could drive to the polls the next day. Mr. Bishop won by about 3,800 votes.

The PAC now plans to use the technique, which is called geofencing, in the run-up to the 2020 presidential election in about half a dozen swing states to find people who may not be registered to vote, said its chairman, Ted Harvey.

"It's another aggressive, on-the-ground effort to get those people identified," Mr. Harvey said.

Democratic and Republican candidates, political parties and outside groups are increasingly tapping into a new source of data as they gear up for the 2020 election: your smartphone. That is allowing for more granular—and sometimes invasive—voter targeting than has been used before.

Armed with this data, campaigns can track down and segment potential voters based on apps they use and places they have been, including rallies, churches and gun clubs. In some cases, voters might see an ad on their mobile phone. In others, companies can match data to a specific person, allowing campaigns to determine who gets a fundraising call or a knock on the door.

Last September, the campaign of then-Senate candidate Beto O'Rourke was able to identify some attendees' mobile device ID numbers during a rally with musician Willie Nelson.

Willie Nelson and Beto O'Rourke at a rally last year.
Photo: Bill Clark/Congressional Quarterly/Zuma Press

A company collected the unique ID numbers of phones that pinged their location while at the event, according to people familiar with the Senate campaign. The company, working with an O'Rourke campaign consulting firm, then matched some of those IDs with contact information, such as email addresses. The resulting list allowed the campaign to follow up with those contacts later on. "It's just a neat idea, and it worked," one of the people said.

Mr. O'Rourke's presidential campaign hasn't so far gathered data this way in his presidential run, people familiar with the matter said.

Political campaigns have long compiled exhaustive lists of all registered voters from state offices or other groups. They later

supplemented that with demographic and purchasing information from data brokers in an approach called “microtargeting” that has been used for years. Now detailed information gathered from smartphones is adding a new dimension to those techniques.

“It’s the marriage of the online and offline data about the individual—that’s the biggest force multiplier,” said Justin Miller, a political data consultant who has worked on campaigns for Barack Obama and Hillary Clinton.

While some are treading more lightly in data collection in the wake of the Cambridge Analytica scandal, in which a data firm tied to President Trump’s 2016 campaign improperly accessed data of Facebook users, others are forging ahead until there is a consensus on where the lines will be drawn.

“I would gladly trade job security for more privacy,” said Mr. Miller. “But since we don’t have it, I’ll keep building models.”

Among the most personal—and powerful—pieces of information available about voters are their location histories.

Track Record

AR

A voter brings a smartphone to a place, such as

a political rally or church.

How your smartphone's location data can end up getting used in a political campaign

“devic
e” : {

An app with location permissions may send the device’s location and a unique identifier to either...

“ifa” :
“59C5BE...C
C79”,

“lat” :
“12.34567”,

“long” :
“8.901234”
}
}

Note: A smartphone app usually has access to location data only if a user has given it permission. Some apps only have permission to send location data when they are being used.

Sources: interviews with ad-tech experts and political consultants; company documents and marketing materials; WSJ app tests

Many popular smartphone applications frequently broadcast their location to an array of online data brokers and advertising companies. It can come through code called software-development kits, or SDKs, hidden inside apps, or as part of the

information that apps auction off to ad companies, testing from The Wall Street Journal shows.

Generally, apps ask for permission to access users’ location, and often may need to be open to transmit that data. Apps get better ad rates—and are sometimes paid directly—when they send this data to advertisers and brokers.

Such precise location data can over time reveal where you live and where you work. It can also lead to more personal insights, such as when you go to the gym, which doctor you frequent or how often you attend religious services. (*See tips on how to limit location tracking below*.)

Companies can tie location data to an individual’s identity by matching an advertising ID number associated with a phone to customer information, or by matching the address a phone pings at night with lists purchased from data brokers.

Textfree, a texting and calling app ranked among the most popular lifestyle apps in the U.S., sends latitude and longitude data, along with a unique ID, to multiple tech companies that help supply ads, including Rubicon Project Inc. and OpenX Technologies Inc., often many times per minute, according to Wall Street Journal testing.

$
$

...a company offering location-tracking services on...

...an advertising exchange to solicit bids, which allows a location-tracking company to tap into its ‘bidstream.’

A political actor, or its agent, works with the location-tracking company, which can have months of historical data.

Online-ad companies use that data to target ads back at the

voter who was at the rally or church.

In some cases, the political actor gets data that can identify people offline—by, say, their home address.

> Attendees wait for the arrival of Mr. Trump at a rally in Rio Rancho, N.M., last month. Photo: George Etheredge/Bloomberg News

Other companies can tap that flow of advertising information, known as the “bidstream,” either directly or through intermediaries, according to industry executives. That allows such companies to track locations over time, or—as in the case of Mr. Harvey’s Committee to Defend the President—draw a fence around a location and identify devices that were there at a given moment.

Greg Woock, chief executive of Pinger Inc., the maker of Textfree, says the company is “clear about advertising in our terms of service” and that users can decline to share their location in their phone settings.

During the 2018 midterm election, the conservative advocacy group CatholicVote drew on information harvested from SDKs in mobile apps to identify people who had set foot in Catholic churches at least twice within 60 days and assigned them a “religious intensity score” based on the frequency of their visits, according to the group and a consulting firm that worked for it. CatholicVote used that information to target roughly 600,000 people with ads for five Senate races, mostly in the Midwest.

One ad in Missouri in support of Republican Josh Hawley for U.S. Senator called his opponent, Democrat Claire McCaskill, “anti-Catholic.” Sen. Hawley won. His 2018 campaign manager, Kyle Plotkin, said the campaign was unaware of the targeting. Ms. McCaskill didn’t respond to requests for comment.

Targeted ads

A political ad campaign against then-Sen. Claire McCaskill of Missouri, sponsored by the PAC CatholicVote, targeted churchgoers using location data.

“It’s no secret that the more often you go to church, generally the more conservative you are,” said Brian Burch, president of CatholicVote, who said the technique was more successful than other methods of targeting Catholics.

CatholicVote and its consultants said they didn’t match names with the smartphone data, only individuals’ home addresses. In the future, Mr. Burch said he hopes to use geofencing to select which volunteers to send to visit which homes. “You’re far less likely to slam the door in the face of someone you’re going to see the next week in church,” he said.

Many apps’ privacy policies say they gather user locations to help target advertising, but the use of such data for political purposes is rarely disclosed prominently, if at all. Data collection from apps is generally legal in most states as long as it is disclosed. The U.S. Federal Trade Commission can investigate if it believes users should have been told more specifically of certain uses of their data, privacy lawyers say.

In the European Union, a new privacy law usually forbids collection of certain types of sensitive data—such as about one's religion, health or political opinions—without explicit consent.

Share your thoughts

What do you think about political campaigns using phone location data to target voters? Join the discussion below.

Several political operatives and campaign officials say they have sought out data from technology companies—including Los Angeles-based Factual Inc. and San Francisco-based NinthDecimal Inc.—that supply location-based services to commercial clients.

Companies commonly use the firms to target ads at people who have visited their stores or those of competitors, or to identify people in the market, say, for a new car because they have visited dealerships.

Factual says it gets location data in large part directly from app developers. It also has its own code integrated into apps such as Perfect365, which allows users to simulate how their faces look in various types of makeup, according to app-intelligence services MightySignal Inc. and Apptopia Inc. Perfect365 sends data to Factual and at least three other location-data firms, Wall Street Journal testing shows, often including users' precise latitude and longitude.

A spokesman for Factual says the company works to gather data only from apps that gather appropriate consent, and has policies in place to stop clients from zeroing in on individuals' identities.

NinthDecimal and Perfect365 didn’t respond to requests for comment.

In 2018, a group opposing a California proposition aimed at curbing profits at dialysis centers used IQM Corp., a political ad-tech firm, to collect bidstream data from mobile phones to target mobile ads to people who visited California dialysis centers a few times a week, according to people familiar with the matter. The proposition failed.

The Committee to Defend the President, the Republican PAC that plans to keep targeting people who attend some of Mr. Trump’s rallies, turned to Louisville, Ky.-based El Toro.

El Toro tells clients that it can pinpoint devices that were in a place going back six months and deliver digital ads to any device in the home of a specific voter, according to pitch documents reviewed by The Wall Street Journal. The company promises to boost turnout by at least 5%, or campaigns get their money back in big campaigns, the documents say.

Users include candidates and political groups on both the left and the right, according to Federal Election Commission records.

Elevate Ohio, a liberal PAC, spent at least $20,000 on El Toro for a few advertising buys in 2018, said Jeff Ruppert, the PAC’s treasurer and counsel. Mr. Ruppert said Elevate Ohio and other progressive PACs he is involved in used El Toro for races including for Democrat Sherrod Brown, who won his U.S. Senate race, as well as losing campaigns for the U.S. House and Ohio’s governor’s office.

Among the locations where the progressive Ohio PACs have used El Toro or similar firms to collect device information were Ohio State football games and political rallies.

Sen. Sherrod Brown celebrates his campaign victory last year in Columbus, Ohio. Photo: Jeff Swensen/Getty Images

Mr. Ruppert said El Toro is among a small group of vendors “that are actually going out and bringing us commercial tools—not just traditional ways to identify past voters.”

El Toro Chief Executive Stacy Griggs says his company doesn’t “provide any raw data back to our customers that would in any way allow them to identify those individuals.” He says he is proud of the company’s political work, which is about 30% of its business in an election year: “Frankly, this type of usage of our

technology makes America better—more voters engaged enough to show up at the polls."

Campaigns and political groups on both sides of the aisle have also used Austin, Texas-based Phunware Inc. to target people who have frequented certain locations in states including Texas, Iowa and New Jersey, according to FEC records and media buyers.

Phunware's website advertises both geofenced advertising and the ability to buy data sets that include location history and mobile identifiers.

"People might get freaked out about this technology," said Democratic political strategist Kimberly Taylor, who said she used Phunware to target people who went to events including the Women's March as part of her work in 2018 as a co-founder of the Fire Ted Cruz PAC that aimed and failed to unseat the Texas senator. "But we're trying to use it for good, trying to engage more people in the process."

The PAC spent about $55,000 with Phunware in 2018, according to FEC records.

The Wall Street Journal asked Apptopia and MightySignal to provide lists of apps that appear to include code from Phunware. The Journal tested several of those apps and found they sent Phunware regular updates detailing users' locations, IP addresses and other device information. One such app is for the Cedars-Sinai Medical Center in Los Angeles, which sent detailed latitude and longitude data, along with a unique device ID, back to Phunware servers during the tests.

Alan Knitowski, Phunware's chief executive, said that the company's data practices are clearly stated in its privacy policy, and that users can opt out by filling out a form on Phunware's website.

Cedars-Sinai said that it is "committed to the privacy and confidentiality of all our patients" and that its "app uses anonymized location data only to help a patient or visitor get from Point A to Point B" on its campus.

Another app sending users' location data to Phunware is GunDealio, a gun-enthusiast deal-finder app. Ryan Gresham of Gun Talk Media, publisher of the GunDealio app, says it has close to 100,000 users with the largest numbers in Texas, Florida and Pennsylvania. The app's terms give Phunware license to use the data it collects, but say nothing about political campaigns.

Mr. Gresham said he was unaware of Phunware's political business.

"Our fans typically don't want to be on a list," he said.

How to Limit Location Tracking

• You can make it harder to associate phone data with your real identity by telling your smartphone to periodically reset a unique identifier known as an advertising ID. (All instructions may vary depending on your phone.)

iOS: In settings, go to "Privacy" then tap on "Advertising." Click "Reset Advertising Identifier." You can also turn on "Limit Ad Tracking," which doesn't stop the use of the identifier completely

but, under Apple's rules, obliges developers to use the identifier for limited purposes.

Android: In the settings app, tap on "Google," then "Ads," then "Reset advertising ID." You can opt out of ad personalization as well.

• You can also limit how apps track and share your precise location. Some apps may not work without location access—such as a map app for directions—but you can often set them to track your location only when they're in use.

iOS: In settings, tap on "Privacy," then "Location Services." Tap on individual apps to select whether and when to allow them to access your location. Then scroll down and tap on "System Services" within "Location Services." Turn off "Location-Based Apple Ads."

Android: Open the settings app. Tap "Location" or, depending on your phone, scroll to "Security & location" or "Advanced" and tap "Location." You can see a list of apps that can access your location. To turn off their ability to do so, tap on "App permission" or "App-level permissions" and select individual apps. On at least some Samsung phones, you'll need to go to "Connections" and tap "Location," where you'll see a list of apps that recently used your location data. After tapping on them, you can disable their location permissions.

Write to Sam Schechner at sam.schechner@wsj.com, Emily Glazer at emily.glazer@wsj.com and Patience Haggin at patience.haggin@wsj.com