ABORTION

Anti-Choice Groups Use Smartphone Surveillance to Target 'Abortion-Minded Women' During Clinic Visits

MAY 25, 2016, 6:52PM | SHARONA COUTTS

Women who have visited almost any abortion clinic in the United States have seen anti-choice protesters outside, wielding placards and chanting abuse. A Boston advertiser's technology, when deployed by anti-choice groups, allows those groups to send propaganda directly to a woman's phone while she is in a clinic waiting room.

Geo-fencing technology can be deployed by anti-choice groups to send propaganda directly to a woman's phone while she is in a clinic waiting room.

Kiva Bay for Rewire

Last year, an enterprising advertising executive based in Boston, Massachusetts, had an idea: Instead of using his sophisticated mobile surveillance techniques to figure out which consumers might be interested in buying shoes, cars, or any of the other products typically

interested in buying shoes, cars, or any of the other products typically advertised online, what if he used the same technology to figure out which women were potentially contemplating abortion, and send them ads on behalf of anti-choice organizations?

The executive—John Flynn, CEO of Copley Advertising—set to work. He put together PowerPoint presentations touting his capabilities, and sent them to groups he thought would be interested in reaching "abortion-minded women," to use anti-choice parlance.

Before long, he'd been hired by RealOptions, a network of crisis pregnancy centers (CPCs) in Northern California, as well as by the evangelical adoption agency Bethany Christian Services.

Flynn's endeavors quickly won him attention in the anti-choice world. He was invited to speak at the Family Research Council's ProLifeCon Digital Action Summit in January this year, and he got a few write-ups in anti-choice press.

In an interview with *Live Action News*—the website for Live Action, the group run by anti-choice activist Lila Rose that is responsible for bogus attack videos against Planned Parenthood—Flynn gave some details about his strategy. He sends advertisements for his clients to women's smartphones while they are sitting in Planned Parenthood clinics, using a technology known as "mobile geo-fencing." He also planned to ping women at methadone clinics and other abortion facilities. His program for Bethany covered five cities: Columbus, Ohio; Pittsburgh, Pennsylvania; Richmond, Virginia; St. Louis, Missouri; and New York City.

"We are very excited to bring our mobile marketing capabilities to the pro-life community," Flynn told *Live Action News*.

Anti-choice groups were tantalized by the ability to home in on the women they think will be most susceptible to their message.

"Marketing for pregnancy help centers has always been a needle in a haystack approach—cast a wide net and hope for the best," said Bethany Regional Marketing Manager Jennie VanHorn, according to the report. "With geo fencing, we can reach women who we know are looking for or in need of someone to talk to."

Flynn's targeting of women seeking abortion presents a serious threat to the privacy and safety of women exercising their right to choose, as well as to abortion providers and their staff, a *Rewire* investigation has found. But

due to weak and patchwork laws governing privacy and data collection in the United States, the conduct appears to be perfectly legal.

Women who have visited almost any abortion clinic in the United States have seen anti-choice protesters outside, wielding placards and chanting abuse. This technology, when deployed by anti-choice groups, allows them to send propaganda directly to a woman's phone while she is in a clinic waiting room. It also has the capability to hand the names and addresses of women seeking abortion care, and those who provide it, over to anti-choice groups.

"It is incredibly unethical and creepy," Brian Solis, a digital marketing expert, told *Rewire,* expressing a view that was unanimous among a dozen experts in digital security, privacy law, and online marketing we interviewed for this story.

Solis said this example was the inevitable application of a technology meant for one purpose—mass advertising campaigns that, while considered by many people to be unseemly and intrusive, do not generally amount to a threat—to a very different, and troubling, objective.

"You can grab an uncomfortable amount of information from someone's device and the apps they use," said Solis. "It's unfortunate, but any woman who plans to visit an affected Planned Parenthood, or anyone who works for Planned Parenthood, should be afraid."

When Ads Follow You Around

By now, most Americans have experienced the following phenomenon: You look at something online—a hotel, a flower delivery service, a course at a local college—and the next thing you know, ads for that thing follow you around the internet for the next week.

A watch you looked at now pops up next to your Facebook feed; an ad for a coffee machine you researched on Amazon now lurks on your favorite news sites. And maybe, after researching cars online, it seems that Toyota knows whenever you visit a lot, and sends ads to your phone as you walk through the dealership's doors.

This is all part of the new landscape of digital advertising, where marketers can tailor their ads to very specific groups of consumers by compiling "personas" based on the thousands of shards of data we all create as we go about our activities online.

While theoretically anonymous, these marketing personas are surprisingly accurate. Marketers likely know your age, gender, occupation, education level, marital status, and—if you have GPS enabled on your phone and are logged into apps that track you—where you live, work, and travel.

What Flynn realized is that he could use the same technologies to infer that a woman might be seeking an abortion, and to target her for ads from anti-choice groups.

"We can reach every Planned Parenthood in the U.S.," he wrote in a PowerPoint display sent to potential clients in February. The Powerpoint included a slide titled "Targets for Pro-Life," in which Flynn said he could also reach abortion clinics, hospitals, doctors' offices, colleges, and high schools in the United States and Canada, and then "[d]rill down to age and sex."

"We can gather a tremendous amount of information from the [smartphone] ID," he wrote. "Some of the break outs include: Gender, age, race, pet owners, Honda owners, online purchases and much more."

Flynn explained that he would then use that data to send anti-choice ads to women "while they're at the clinic."

In his sales PowerPoint, Flynn said that he had already attempted to ping cellphones for RealOptions and Bethany nearly three million times, and had been able to steer thousands of women to their websites. The price tag for one of Copley's campaigns, he said, was $8,000.

Flynn initially agreed to speak with *Rewire* for this story, but did not respond to multiple follow-up emails and phone calls. Much of this report is based on materials that he sent to people he believed to be potential clients. Numerous messages seeking comment from management for RealOptions went unanswered; Jennifer Gradnigo, a spokesperson for Bethany Christian Services, confirmed that they have used Copley's services and "appreciate their ideas," but declined to discuss specific campaigns.

Not everyone who received Flynn's pitch emails was impressed. One recipient contacted *Rewire* after speaking with Flynn, and expressed horror at what Flynn told her he was able to do on behalf of anti-choice clients.

"I felt disgust, and I felt protective of these women who are going to seek

sensitive medical services at a time when they're vulnerable," said the recipient, who is a social worker at a Northern California adoption agency. *Rewire* agreed to withhold her identity due to her fears of retaliation from anti-choice activists.

"They're being spied on by this capitalist vulture who is literally trying to sell their fetuses," she said. "To do this to women without consent is predatory and it's an invasion of her privacy, and unethical."

In emails and PowerPoint presentations sent in early March, Flynn claimed to have reached more than 800,000 18-to-24-year-old women on behalf of RealOptions, and to have sent more than 2,000 of those women to RealOption's website.

Rewire obtained three examples of the ads that Flynn said he had sent to young women's phones on RealOptions' behalf.

The ads are typical of CPCs.

They ask, "Pregnant?" or "Abortion?" and then include statements like "It's your choice. You have time… Be informed" and "Get the facts first."

Like most CPCs, the claim that RealOptions provides "facts" about abortion is deceptive. While that language may lead women to believe they could obtain abortion care at RealOptions, in federal tax filings, the organization explains its mission as: "empowering and equipping women and men to choose life for their unborn children through the love of Jesus Christ in accordance with his word regarding the sanctity of human life."

According to its website, RealOptions has received funding from the radical Christian group Focus on the Family. The organization was founded in 1981 by Marion and Tom Recine, fervent Christians who in a video posted to their website refer to the "many, many, many women who've come to Jesus because of the [RealOptions] centers."

Flynn also says that he has targeted 140 abortion clinics on behalf of Bethany Christian Services over the past few months, and that 10,000 people clicked on the ads for Bethany that he sent to smartphones in those clinics, directing them to a "dedicated resource centers landing page."

page.

Bethany is the nation's largest adoption agency, with assets of more than $45 million in 2014, according to the most recent available figures. The chain has faced accusations of pressuring birth moms to continue pregnancies against their will, of abandoning mothers who change their minds and decide not to go through with adoptions, and other abuses.

The social worker who received Flynn's pitch deck told *Rewire* she was alarmed that Flynn had succeeded in reaching so many women on behalf of his anti-choice clients.

"He's doing it and it's working and it's probably really impacting human trajectories," she said. "It changes human lives to be funneled into a system like this."

Advertising Is Now a System of Surveillance

Although it is now ubiquitous, mobile digital advertising is a relatively new phenomenon, only as old as the sophisticated smartphones on which it relies. As a result, laws and the regulators who enforce them are lagging behind when it comes to the many possible ways that bad actors can abuse smartphone advertising.

In terms of federal laws, many either don't apply to Flynn's conduct, or would allow it, according to Chris Hoofnagle, a professor at the University of California, Berkeley's School of Law, and School of Information.

"Privacy law in the U.S. is technology- and context-dependent," Hoofnagle said. "As an example, the medical information you relay to your physician is very highly protected, but if you go to a medical website and search for 'HIV' or 'abortion,' that information is not protected at all."

In other words, it's almost certain that the Health Insurance Portability and Accountability Act, known as HIPAA, would not apply.

The other limitations, such as they are, come from two sets of laws. The Federal Trade Commission (FTC) and state attorneys general can prevent advertisers from sending false and misleading ads; they can also stop advertisers from lying about what information they are tracking and what they plan to do with it once collected.

The FTC did not reply to *Rewire's* questions in time for the publication of this story. However, the commission does not have jurisdiction over nonprofits, so it is highly unlikely that it could take action in this case.

The second set of laws concern user consent. Companies like Verizon and AT&T, known as carriers, are required to get affirmative consent before using "Customer Proprietary Network Information" gleaned through cellphone towers—including call records and location—for marketing. Apps don't use network information, but rely instead on the GPS built into phones. They also need to obtain affirmative consent to collect and use information for marketing.

Obtaining that consent is easier than many consumers may think.

"The reality of this stuff is that no one's asking what marketers will do with their information when they click, 'I Agree,' when an app asks if it can use their location," Hoofnagle said. "If one consents to that tracking, and consents for it to be used for advertising purposes, that's pretty much the end of the story."

Certainly, most people wouldn't imagine that by agreeing that, say, Yelp, Snapchat, Tinder, or the *New York Times* could use their location, that marketers could then use the same information for the very different purpose of figuring out whether they are seeking sensitive medical services.

Hoofnagle says that such use is perfectly legal, as long as companies don't lie about what information they're collecting—even if those disclosures are buried in fine print.

For his part, John Flynn is confident that his campaign is within legal bounds.

"I have worked with pharma, medical recruitment and many others where we mobile geo-fenced medical centers without a problem," he wrote in an email to a potential client. "Bethany's campaign targeted just medical centers and there was [sic] no issues. RealOptions in the San Jose area is presently targeting colleges and medical centers without issue."

In the absence of robust legal limitations in the United States, advertisers have organized into self-regulatory bodies to police themselves, acutely conscious that examples of egregious privacy violations could spark a public backlash, and lead consumers to block ads and to opt out of targeted marketing.

Lindsay Hutter, a spokesperson from the Direct Marketing Association (DMA)—a New York-based group that represents direct marketers—said in

an email statement to *Rewire*:

> A key pillar of DMA's work is to ensure that data-driven marketers conduct their work on an ethical basis, respecting the private information of consumers. This is particularly true for sensitive medical information about particular individuals, the use of which for marketing purposes without permission is against DMA's Ethical Guidelines. Any location-based marketing should be opt-in, with the consumer notified that marketing offers are being presented due to their location.

Hutter did not provide a direct reply to our questions as to whether targeting women who might be seeking abortion care on behalf of anti-choice groups would be in violation of DMA's guidelines.

It would, however, violate Facebook's standards, according to Tom Channick, a company spokesperson.

"Our policies prohibit ads that make implications, directly or indirectly, about a user's personal characteristics, including medical condition or pregnancy," Channick said. "Deceptive or misleading advertisements are also prohibited."

Flynn claims that he has a "relationship" with Facebook that allows him to "place mobile and digital ads in Facebook pages," but Channick said the company could find no record of Flynn or his company ever using their platform.

Calling Flynn's campaigns "really objectionable," Hoofnagle said that these kinds of practices are toxic to the digital advertising industry, as well as the platforms—like Google and Facebook—that depend on advertising dollars.

He said this example drives home the fact that the nature of advertising has fundamentally transformed with the rise of the internet, and as smartphones have become ubiquitous.

"Advertising is a system of surveillance now," Hoofnagle said. "It used to be billboards and television. Now it's surveillance."

Extremists Could Use Women's Phones to Learn Their Names and Addresses

Surveillance has long played a central—and deadly—role in the efforts of anti-choice activists to intimidate women out of accessing abortion care

anti-choice activists to intimidate women out of accessing abortion care, and to stop providers from making it available.

In the late 1990s, an anti-choice extremist created a website called the Nuremberg Files—in reference to Nazi Germany—which was a list of the names and addresses of doctors who provided abortions. Operation Rescue maintained a site called "Tiller Watch" that monitored the doctor's whereabouts until he was murdered in the spring of 2009. Extremists have published "Wanted" signs with photographs of abortion providers. Activists in Texas stalk people entering local clinics, noting their physical appearance and license plates, hoping to determine which women went through with their abortion and whether anyone changed their mind, as well as to identify clinic workers. Many providers around the country report having been followed on their way to and from work.

Sasha Bruce, senior vice president of campaigns and strategy at NARAL Pro-Choice America, says that tagging the cellphones of women who go to abortion clinics falls within the pattern of intimidation.

"Intimidation frankly is the lowest threshold—that quickly turns to violence," Bruce said. "That's part of what's troubling about this. There's a real incitement that this information can contribute to."

Bruce said she was alarmed in particular because Flynn was not just collecting information about what women looked at online, but also about their physical locations.

"If you have the smartphone ID, and then you can tie that to a location outside of the clinic, let's say a home, that's a real security threat," Bruce told *Rewire*. "I worry about the extension of that—the desire of anti-choice activists to know who these staffers are, and who the women are."

To be clear, there is no evidence to suggest that Flynn or his clients have or want to use geo-fencing to learn the real identities of women seeking abortion. But experts told *Rewire* that the potential for others to abuse the technology is a cause for alarm. In keeping with the view that transparency fosters security, *Rewire* has chosen to outline the ways this tracking could be misused.

In theory, when marketers gather information about individual smartphone users through methods like geo-location, that data is anonymized, meaning that it is not attached to a person's name, but rather to a unique number known as an "advertising ID." That is the number associated with the particular copy of the operating system that each of us has

the particular copy of the operating system that each of us has downloaded onto our smartphone. If you use a Google phone, your operating system is Android; for iPhone users, it's your copy of iOS. Much of what you do on your phone can be associated with that advertising ID.

In most cases, marketers want to collect data from millions of potential customers, said John Deighton, a professor of marketing at Harvard Business School, in an interview with *Rewire*. The more data they have, the more ads they can send, which enhances their database.

"What your story is drawing to my attention is that these same surveillance technologies can be used at a much more micro scale," he said. "You could imagine outright illegal use of geo-targeting: for example, geo-targeting a rich person's house and getting an alert when they leave home." That could, say, lead to high-tech burglary.

"Once you start realizing you can target desirable individuals, instead of being a big data function it becomes about tiny data," Deighton said.

But if all of the data that marketers collect is supposed to be anonymized, how could bad actors—including anti-choice extremists—figure out the actual identities of the people they track?

The dirty secret of digital marketing is that it is in fact relatively easy to find out the real identities that are attached to our online IDs, according to experts who spoke with *Rewire*.

The most obvious way is simply to ask people for that information.

Both RealOptions and Bethany Christian Services require a person's name and contact information in order to receive information online. Once a woman enters her name, email, home address, phone number, or ZIP code, that information is tied to her advertising ID, and Flynn could potentially marry that ID to all data associated with it and store it in what he calls his databank.

There are, however, plenty of less aboveboard methods to learn the name attached to an anonymous ID.

Any site or app that uses a profile with your name and any other information—Facebook, dating services, banking apps—can link your device, and your advertising ID, to the real you.

Legitimate services would not hand over personally identifying information willingly, but there are many instances of such information being made

widely available. The cyber attack on Ashley Madison, the dating site for married people seeking extramarital partners, resulted in the release by hackers of the personal information of 32 million of the site's users, revealing the potential for profile-based sites to be targeted.

Even without sophisticated hacks on established sites, bad actors can use techniques known as "social engineering" to learn the personal identities associated with advertising IDs.

For instance, if an anti-choice group wanted to learn the identity of women seeking abortions, instead of sending them ads for CPCs, they could send ads that seemed unrelated to abortion—for a competition to win $500, or for help with student loans—that tricked women into entering their names, email addresses, and any other information required by the form. Any woman who filled out the form would have unwittingly handed her name to anti-choice activists.

That would allow anti-choice groups to literally see women's whereabouts in real time, said digital marketing experts who spoke with *Rewire* anonymously because they were not authorized to speak with the press. They described marketing software that allows them to see targeted individuals' locations, the same way you can see yourself as a blue dot on a smartphone map. If certain people were seen at an abortion clinic regularly—say, during work hours—Flynn or his clients might even be able to infer that they work there.

"That's what scares me about your story," said Deighton. "Now we have an incentive to track people that isn't the usual big data incentive."

The question naturally arises: What can abortion providers and the women they serve do to fend off these digital affronts?

The simplest measure Planned Parenthood, or any other abortion provider, could take is to tell patients to leave their smartphones at home or in the car. If that isn't possible or practical, the best advice is to turn off their GPS and log out of all apps before they come to a clinic.

It's a simple step, but one that many people either won't or don't take, said Cooper Quintin, a technologist at the Electronic Frontier Foundation (EFF), a San Francisco-based organization dedicated to preserving fundamental rights in the age of technology.

"The way we need to fight back against this is by blocking these things that

are tracking who we are and where we are and what things we're looking at," Quintin told *Rewire*. EFF considers location-based tracking to be a serious threat to privacy.

"Right now, there's this big ideological debate about ad-blocking. What's missing from that debate is the idea of blocking things that are tracking you. Tracking people and building up these databases of what they read online, where they go in the real world, linking their online behaviors to their offline purchases and real world behavior—these things can have real-world effects, and this is a horrific example of how this can affect people in a way that's much more important than seeing some annoying or creepy ads that follow you around."

Editor's Note: Watch our video for info on how to avoid location-based tracking.