SNIPER AD TARGETING

Marc Faddoul
School of Information
UC Berkeley
marc.faddoul@berkeley.edu

Rohan Kapuria
School of Information
UC Berkeley
rohan.kapuria@berkeley.edu

Lily Lin
School of Information
UC Berkeley
lilyelin@berkeley.edu

May 10, 2019

ABSTRACT

The digital ad infrastructure is getting increasingly powerful and precise at targeting users with more 'relevant' content. Ads are customized with granular behavioral and demographic data. Cookies enable advertisers to re-targeted users across devices and sessions, and audiences defined by personally identifiable information bridges the gap between online and offline marketing. These developments are beneficial to the internet industry, but also enabled the emergence of a dangerous practice called *Sniper-Targeting*.

Sniper-targeted campaigns exploit micro-targeting criteria in order to reach a pre-defined audience with tailored content. As information warfare intensifies on the internet, this practice can be a powerful method to manipulate, extort private information, and back cyber-attacks. This paper reviews how sniper-targeting has been used in the past and how it evolves in the current landscape. We investigate different sniper-targeting strategies, including using Facebook's *Custom Audience* feature and a new tool that claims to make sniper-targeting available to the masses. Despite limitations, we show that sniper-targeting is relatively easily achievable and that preventive measures will be required to limit the spread of this phenomenon.

Contents

1 Introduction

The internet is underpinned by a sophisticated micro-targeting and re-targeting infrastructure aimed at serving more relevant and personalized recommendations to consumers. To pursue that goal, the digital ad ecosystem is constantly being refined with richer data and more effective technology, such as with Facebook's introduction of *custom audiences* [1], a feature that allows advertisers to directly upload a list of customers so that they can be targeted on the platform, bridging the gap between online and offline marketing campaigns. Albeit being poorly understood by users, it is generally expected that ads are targeted at the aggregate rather than at the individual level.

The same infrastructure can be used by motivated actors to send an individually-tailored ad to a specific person, often will malicious intentions.

The practice, called sniper-targeting was first pointed out in 2010 as a vulnerability on the Facebook ad platform, after which the company allegedly fixed the bug [2]. Several subsequent instances have been reported since then. Sniper-targeting is becoming more common, as a turnkey service makes it readily available to the masses [3]. This concerning trend supports the escalating weaponization of the digital ad infrastructure [4]. In that context, we aim to:

- Identify the instances of sniper targeting which have been documented
- Describe relevant contextual elements of the landscape in which this practice fits
- Define the specificities of sniper-targeting and the risks they entail
- Cite legal frames that are relevant to evaluate this new practice
- Explore and test the current possibilities to perform sniper-targeting, directly from the ad platforms or using a 3rd party service
- Provide recommendations to users, policy-markers and to the industry to contain sniper-targeting

2 Sniper Targeting Instances

In 2013, a sword-swallowing practitioner went on Facebook and saw a strange ad that said: *'Does it seem ironic that swallowing a sword is easy and then small pills make you gag?'*. He had never specified that he struggled swallowing pills anywhere online, or even in private messages. Indeed, he freaked out. It is only after receiving several of these creepy targeted ads that he realized that this was all a prank from his roommate [5].

The story went viral [6], and exposed to the internet a technique which had already been described in the 2011 book 'Likeable Social Media', where the author explains having used sniper-targeting to send a love message to his wife [7]. It was not specified whether she found the enterprise likeable.

This Facebook vulnerability had been aired in 2010 by Aleksandra Korolova's [2]. She had investigated how the ad platform could be directly used to target an ad to a single specific individual. After communicating her findings to Facebook, the company launched a change to their system, establishing a lower bound of 20 people for campaign audiences. In this pioneering paper, Korolova had already warned that this safeguard was insufficient and could be circumvented. Several subsequent instances of sniper-targeting on Facebook proved her right.

The strategy started being used for other purposes than joking with friends and relatives. In a medium post, an ad agency brags about using sniper-targeting to push discrete and individually tailored ads to commercial leads to convince them to seal a deal. It explains how the agency sometimes embed the logo of the prospect's company in the ad in order to better catch the eye [8]. In an other blog post, a real-estate agent affirms using the same technique, which he calls '*Facebook advertising on steroids'*. He explains that *'the goal is to try and be very specific without being too obvious and looking like a stalker'* [9].

Besides sneaky marketing, sniper-targeting was instrumentalized to manipulate. Head of UK-labor party Jeremy Corbyn was sniper-targeted by his own campaign staff, who thought the ads their boss had ordered to run were too far left in order to resonate. They targeted the ads they had been instructed to broadcast only to Corbyn and a few other officials

who were looking for them, while they blasted more centrist ads to the rest of the audience [10, 11]. More comically, John Oliver has allegedly been buying ads on Fox News specifically hoping that Donald Trump would see them and change his views about the Iran nuclear deal [12]. The potential of sniper-targeting has also found its way into TV shows. In an episode of The Good Fight [13], a plucky legal aid creates an advertisement for a fake art show and beams it only to one judge, who is ruling whether an undocumented immigrant is a noted artist and so should be granted a visa.

Sniper-targeting manipulation can deeply change an individual's life, as illustrated by the enterprise of a disillusioned ex-Mormon [14]. Jones had been convinced to leave the church after reading an open letter detailing historical details and controversies about the LDS's church, that are usually unheard of in the Mormon community. He wanted to share it with his wife and relatives, but they were unwilling to read what was considered to be 'anti-Mormon propaganda'. He therefore leveraged his expertise on the Facebook ad platform to send his wife the compromising text disguised as an article preaching the magnanimity of LDS church founder Joseph Smith. The plan was stunningly successful: his wife clicked on the orthodox-looking ad, and got redirected to a website his husband had put up just for her. Once she started reading it, she couldn't stop. *She stopped believing a couple of days after that*, Jones said. He sent the same ad to a few other friends and relatives who'd turned away from him after he left the church, and had impact on several. It was so successful, that Jones started a project to help other disillusioned ex-Mormons do the same. Despite the fact that the ad was sent to several individuals, this example is a quintessential example of sniper-targeting which illustrate the potential for this technique to manipulate relatives sometimes with tremendous impact.

In all these examples, the attack was performed by online advertising specialists, who are familiar with the tool and well motivated to perform the attack. Last year, a tool was put on the market, offering a sniper-ad targeting service for 30$, which does not require any technical knowledge. The service offers some turnkey manipulative campaigns aiming at convincing a colleague to quit their job or inciting one's partner to initiate sex. Tailored campaigns are also offered [3, 15].

Almost 10 years after having been first reported and denounced, sending an add to a single and specific individual remains possible (particularly on Facebook, see 6.1) and is becoming more common. Step-by-step instructions guides and ready to use services make sniper-targeting available to the masses. This trend adds up to the long list of malicious strategies with which the ad infrastructure is being abused, and amplifies several existing concerns in the current digital advertising landscape.

3 The digital Advertising Landscape

3.1 Current Controversies Regarding Micro-targeting

The advertising infrastructure has been continuously developed and refined in the last decades in order to become more efficient at matching content with users [4]. These 'improvements' were driven by:

- Sprawling consumer monitoring systems to gather data [surveillance capitalism]
- Increasing abilities to target specific audiences across channels and contexts
- Automated feedback loops allowing to further refine the content, layout, timing and placement of an ad for a specific audience

The collective discourse of advertisers to justify these means is that targeted advertising benefits everyone by making ads more relevant, including users since more relevant is allegedly less annoying [16]. It also allows many services to remain free of charge for the user. As Google's Chief Legal Officier stated before Senate, *'Simply put, advertising is information, and relevant advertising is information that is useful to consumers'* [17].

Though, there is a growing debate as whether more 'relevance' is beneficial for the consumer. Despite the privacy concerns which stem from the data gathering processes, the ads themselves can entail adverse consequences to whom they are served.

Indeed, ads can promote products that are undesirable. For instance, pay-day loans are harmful to most borrowers and are illegal or restricted in many states. But reckless advertisers leverage the micro-targeting infrastructure to target vulnerable individuals who could be interested in outrageously high interest loans, even in locations where it is illegal [18].

Not seeing certain ads can also be detrimental - discrimination on protected attributes is a common criticism. Black and hispanic kids are for instance disproportionately targeted with junk food ads [19]. Facebook was sued by the ACLU for allowing discrimination against women on job advertisements [20], and by the U.S. Department of Housing and Urban Development for allowing race discrimination on housing ads [21]. Jobs and housing ads have special legal frames which constrained the platform to make changes in both cases [22, 23], but these can easily be circumvented using other criteria as proxy for protected attributes [24].

Micro-targeted ads can also be invasive, offending, or creepy. Compilations of user feedback illustrate how context specific advertisement has become so performant that many became convinced that their devices are listening to them [25]. This belief is in practice highly unlikely [26]. Nonetheless, users are often feeling breached into their privacy and sometimes offended by inappropriate ads, such a user who reported being bombarded by incontinence pants since they turned 60.

More injurious, is the use of targeted advertising for harassment. Geo-fenced advertising has been reported to be used to serve anti-choice campaigns to women located in an abortion clinic. As this example highlights, not only can micro-targeting be used to drive sales, but also to drive influence and political discourse.

3.2 Ads Drive Influence, Not Just Sales

The micro-targeting infrastructure was developed with exceptional commercial incentives. In 2017, internet advertising revenues totaled $88 billion just in the US [27]. The business models of Google and Facebook almost entirely relies on their ability to rely on their ubiquitous platforms and databases to better target consumers. But are ads really only trying to target ‘consumers’?

During the 2016 US presidential election, $1.4 billion dollars were spent in digital ads, a staggering 789% increase from 2012 [27]. Increasingly, governments, interest groups and regular citizens around the world leverage ads an digital media to artificially shape public life. These emerging practices of digital misinformation and manipulation are referred to as ’computational propaganda’. Whistle-blower Christopher Wylie who participated within Cambridge Analytica to a micro-targeting campaign fueled by a maliciously-gathered database of millions of Facebook users explained to the Canadian parliament:

> *"The problem with targeting is that rather than standing in that public forum, you are going to each individual voter and whispering something in their ear. Now, in many cases what you’re whispering is something you would be happy to say in that public forum. In some cases, it may not be."*

Cambridge Analytica’s interferences in the Brexit and the 2016 American presidential campaigns are two instances of computational propaganda which have been extensively covered in the media. But these are just the tip of the iceberg. From Azerbaijan to the Philippines, states and influence groups are building digital influence armies all around the world [28]. Targeted ads are crucial elements in their arsenals, as they allows well funded actors to scale up their propaganda efforts.

These ads can be used as a soft-power instument, for instance, to broadcast content from affiliated media. They can also be exploited more bluntly to silence dissident opinions. For instance, lobby groups have used Facebook ads to run defamatory campaigns targeting Palestinians-right activists on American campuses [29], including at UC Berkeley [30, 31].

The potential of the advertising network need to be reevaluated in the light of these new influence wielding practices, which are very different from the commercial purposes it was designed for. This is particularly concerning considering

that targeting possibilities have become optimized not only in order to fulfill the declared goal to better match consumers with services, but also to discover and exploit cognitive vulnerabilities.

3.3 Digital Ads Leverage Behavioral and Psychological Exploits

The field of behavioral economics, which studies the systematic cognitive biases with which humans differ from a purely rational behavior has strongly influenced digital marketing [32].

A marketing study advises cosmetic companies to target women during *prime vulnerability moments* such as Monday mornings where women *feel less attractive* [33]. This strategy does not make the ad more relevant, but does increase the click rate. Under such click-rates performance criteria, vulnerability is indistinguishable from relevance. Since the algorithms underpinning ads distribution are optimized for click-rate metrics, cognitive exploits are systematically discovered and leveraged, which have made them ubiquitous.

This use of the ad infrastructure to automatically identify and target weak points where groups and individuals are most easily influenced is a form of weaponization [4]. And as data keeps flowing, algorithms become increasingly effective at exploiting human vulnerabilities, and the weapon increasingly powerful. This can be a concerning when ads are used for commercial purposes, as illustrated above with the Monday morning cosmetic targeting. These concerns take a whole new dimension when the intention of the advertiser shifts from driving sales to driving influence.

Cambridge Analytica's, backed by their Behavioral Dynamics Institute research, heavily relied on behavioral economic insights to run their large scale political influence campaign in 2016. But they added yet another layer of refinement for finer customization. Cambridge Analytica combined OCEAN personality tests with data mined from social media to generate "psychographic profiles" for every adult in America in order to predict their personality traits. This was the first time the general public was exposed to a widespread use of 'psychological targeting' in political campaigns [34].

4 The Impact of Sniper Targeting within this landscape

4.1 What is fundamentally new?

It is tempting to define sniper-targeting as the edge-most form of micro-targeting, where the audience is reduced to a segment-of-one.

Reaching the segment-of-one has been a lingering gold-standard for marketers for decades. Back in 1989, an article from BCG consulting firm stated: *"The foundation for "Segment-of-One Marketing" is the ability to track and understand individual customer behaviour. Thanks to the expansion of data capture opportunities and lower storage costs, such databases are already cost-effective on a large scale"* [35]. The goal of this endeavor was *the ability to perform to exacting service standards at the customer's convenience.* In that sense, the customer is only defined by his behavior as a consumer.

In 30 years, reaching such 'segment-of one' has become common practice. Let's consider these 2 scenarios:

1. A rural musical instrument shop is trying to sell a large didgeridoo they have in stock. The owner puts up a Facebook ad targeted at 'Didgeridoo Players' within a radius of a few miles around the shop. Only one person matches these criteria and gets targeted by the ad.
2. An eccentric individual craves a slice of square watermelon. He looks up 'buy square watermelon' on Google and subsequently becomes the first and only person to receive an Amazon ad for square watermelon seeds.

In both cases, the ad was targeted at a 'Segment-Of-One'. The first scenario illustrates that 'people like me' can in fact be just me. The second illustrates that cookies can be leverage to automatically customize ads at the individual scale. Though, it seems that most people are comfortable receiving such ads, unlike the cases of sniper-targeting described above.

Therefore, an audience of size one is neither sufficient for an ad to be sniper-targeting, nor necessary, as in the anti-Mormon propaganda example detailed above [14]. Rather than the size of the audience, the fundamental distinction between sniper-targeting and micro-targeting in that the audience is targeted for their specific identity, not for their personal characteristics or online behaviors. This draws the distinction between traditional micro-targeting and what we define as 'sniper-targeting'.

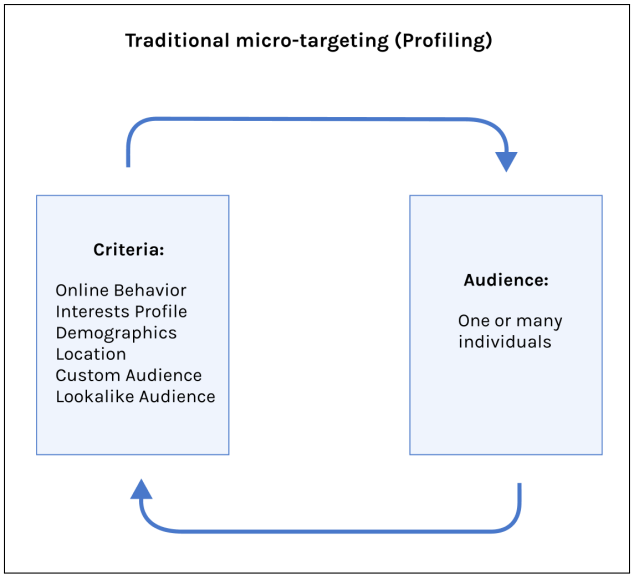


Figure 1: In micro-targeting, the criteria defines the audience. In sniper-targeting, the audience defines the criteria.

In traditional micro-targeting the advertiser uses a set of criteria in order to profile an audience (shown in Fig. 1). If several people constitute the audience, there are no prior preferences for one individual over another. The audience is defined by the criteria.

In sniper-targeting, the criteria are set in order to reach a pre-defined audience. If several criteria combinations allow to profile the exact same person(s), there are no prior preferences for one criteria combination over another. The criteria are defined by the audience.

In sniper-targeting, the intention of the advertiser is to reach a specific identity, not a specific profile. **We define a sniper-targeting campaign as one which exploits profiling criteria in order to reach a pre-defined audience.**

4.2 Why does it feel wrong?

The definition suggested above focuses on the technical implementation of the campaign, but does not describe what makes sniper-targeting feel 'wrong' or 'creepy' as opposed to traditional micro-targeting. We suggest two main drivers for these feelings.

Misalignment with user expectations: Ad targeting strategies are expected to be defined at the group aggregate level, not at the individual level. If the ad is individually customized, it is expected to be done in an automatic fashion based on data collected from the use's online behavior, as with ads featuring a specific flight and date after a booking process has been dropped in the middle. In instances of sniper-targeting, these expectations are violated. The ad is specifically sent to a single or small group of individuals, and customized based on information that may have been obtained offline and that is typically not available to advertisers. As with privacy concerns, the fact that the practice feels 'wrong' or 'creepy' stands from an expectation misalignment [36].

Ill-intentions of the advertiser: The second driver for the 'creepiness' comes from the receiver interpreting the intentions of the sender. Indeed, why would someone try to send a sniper-targeted ad in the first place? Sending a

sniper-targeted ad to someone requires a significant amount of information about that person, such as an email address, a phone number, a physical address or detailed lists of interests and demographics. This information gives plenty of options for the advertiser to communicate a message to the individual, if they are willing to hear it. Therefor, the point of sending a sniper-targeted ad instead of using another media is for the advertiser to either conceal their identity and intentions (ie to manipulate) or to force through a message that the individual refuses to receive (ie to stalk or harass). The fact that sniper-targeting can often only be motivated by ill-intentions reinforces the negative view about this practice.

4.3 Current and Fore-coming Risks?

Instructions available online and turnkey services make it easy for anyone to perform sniper-targeting. There is a strong potential for these tools to become more powerful and more accessible. This increasing availability is concerning for three main reasons:

Widespread malicious ads: The use of sniper-targeted ads for deceptive and manipulative purposes confirms that the digital ad infrastructure can be hijacked off commercial intents to more malicious ones. The strategy can also be exploited to harass an individual or to carry defamation campaigns.

Privacy Threats: When a link sent with a unique identifier through a sniper-targeted ad is accessed, the data collected by the cookie of the website can be matched with the target's identity, certainly violating privacy expectations and potentially the law. It was shown that sniper targeting could be used to exploits the Audience Insights tools into leaking profiling information about the target [37, 38]. Indeed, as users, these tools are designed with expectation that the audience to be relevant at the aggregate level, not the individual. The tool needs to be reassessed to include constraints of differential privacy.

Phishing and Social Engineering: Sniper-targeting can be a potent vector for cyberattacks. A phishing link can be sent via an ad to a specific target. The potential for sniper-targeting ads to support manipulation and information leaks can also back social engineering attacks.

5 Legal Frames

Some have described sniping campaigns as a form of subliminal messaging [39]. The idea is that ads can follow you around the web, planting ideas or subconsciously manipulate the target into some form of action. However the legal definition of subliminal communication is

> *"the projection of messages by light or sound so quickly or faintly that they are received by the listener below the level of conscious awareness."* [40]

Being currently mostly fixed text and image based advertising elements, current target sniping campaigns falls within the supraliminal domain. However given typical browsing behaviors, users can scan quickly largely ignoring areas of the page traditionally associated with advertising, one should think more carefully about whether or not online advertising might take on subliminal qualities through the combination of placement and user behaviors. We will proceed in our analysis assuming that target sniping is not a form of subliminal communication.

The legality of target sniping currently can depend upon how it is technically conducted.

5.1 Europe: GDPR

Article 3 of the GDPR prohibits the processing of personal data or the monitoring of user behavior for a subject located in the EU. This means that if a person is in an EU country, you cannot serve ads base upon their search history or previous web activity. Companies are not prohibited from collecting personal data or behavioral information from

a person in the EU, however if they do so, they then need to abide by GDPR requirements which include providing transparency to users in clear language, allow users the right to access their data, object to data processing, and right to be forgotten [41].

Given the goal of target sniping is to identify and serve a single individual with targeted advertising, ideally without them knowing they are being advertised to in a segment of one campaign, it is hard to imagine a version of target sniping that would be legal under the GDPR. It also brings up an interesting dichotomy where a company seeking to serve ads to an user in the EU would have to construct a system that protects privacy, must ensure that all data collected is can be identifiable for accessibility or for erasure (right to be forgotten) upon request of the user.

There is a current complaint filed against Google that argues the current ad bidding process, where advertisers bid upon target audience segments based on characteristics of their personal data, is in violation of Article 5, paragraph 1 [42]. Methods that rely on retargeting most likely will require consent [43]. Cookies are considered identifiers under the GDPR Recital 30 and thus methods that involve cookies would also need to first obtain consent from the user. It is unclear what level of transparency or informed consent needs to be gotten, whether consent to use cookies is sufficient or the specific activity involving cookies necessitates consent getting.

5.2 United States: FCC and CPA

In comparison to Europe, the United States appear to move in the opposite direction. Unlike the Europeans that old content distributors and advertisers accountable, the FCC has released privacy guidelines for ISP but notably leaves out content distributors and advertisers. ISPs are not allowed to provide a list of "sensitive data" without consent which includes items such as precise geo-location, health and financial information, social security numbers, children's information, web browsing history, app usage history, and content of communications.

While the FCC is ruling that the ISP needs to stay clear of data that could be used in targeting advertising, it is supporting efforts to allow more targeted advertising at the endpoints. Next Gen TV transmission standard 'ATSC 3.0', reported to be the "world's first Internet Protocol (IP)-based broadcast transmission platform was greenlit by the FCC in 2017. The transmission standard is supposed to allow broadcasters "to provide more targeted advertisements to individual viewers [44, 45]. In short, if you are not an ISP and the endpoint is a TV, you are allowed to do individual targeted advertising.

There are no clear regulations against targeted advertising in the United States and some forms of targeted advertising are even supported. Even if sniper targeted were to be considered subliminal advertising, there are no formal rules on "subliminal" advertising. The closest is a 1974 policy statement that says the use of "subliminal perception" is "contrary to the public interest" [46].

There does exist other legal risks that targeted sniping could transgress due to its unique nature. For example, there are spatial regulations, "bubble zone" or "access zone" to protect access to abortion clinics that prohibit protests within a certain distance [47], temporal regulations, e.g. political solicitation is prohibited within 100 feet of the entrance of a polling place on primary or election days [48].

Lastly, the recent California Privacy Act does afford residents of California a few more protections including the right to opt out of the sale of their data, disclosure, deletion, access, and non-discrimination [49]. Unlike the GDPR, there is nothing in the CPA that indicates targeted advertising will be constrained directly, however several of these rights, e.g. disclosure, access, could have an impact on targeted advertising.

6 Investigating Sniper-Targeting Strategies

This section explores different technologies that can be used to perform sniper-targeting.

1. **Facebook Custom Audiences**: We investigate the use of Custom Audiences on the Facebook Ad platform, a sniper-targeting technique which has been found successful in the past. [Korolova2018]

2. **The Spinner**: We investigate the turnkey sniper-targeting service by following its effectiveness on a targeted individual and analyzing the underlying cookies.

3. **Other Strategies**: We discuss the potential for other strategies to work, such as malicious browser extension or keyword targeting on Google Ad-Words.

6.1 Facebook Custom Audiences

6.1.1 Context

In 2010, Korolova alarmed Facebook that *the variety of permissible targeting criteria allows micro-targeting an ad to an arbitrary person*. [2] This was the first time that sniper-targeting possibilities were brought to light, as well as the risks of information leaks that this practice entails. This led Facebook to implement a change to their ad platform, setting a minimal audience size to 20 users, allegedly a hard threshold.

Korolova already warned at the time that this safeguard could be circumvented. She was proven right, as many of the real-life examples cited in Part II combined Facebook filtering criteria with *Custom Audiences* to perform sniper-targeting. This feature, as well as Google's equivalent *Customer Match Audience* or Twitter's *Tailored Audience* are generically called 'Personally Identifying Information Audiences' [50]. They were introduced to bridge the gap between online and offline marketing campaigns [1], allowing advertisers to directly upload a file of customers to create an audience on the platform. Facebook allows to match user profiles based on a variety of personal identifiers such as name, phone number, email ID, gender, or age [51]. Korolova alerted Facebook again about the vulnerabilities of this feature in 2018.

6.1.2 Study Design

Research Goal: We aim to explore whether and how Facebook Custom Audiences can still be exploited to perform sniper-targeting.

Implementation: We run two campaigns on the platform as described below. Table 1 gives the full criteria of these two campaigns.

- **Campaign 1:** We create a Custom Audience with 27 males and 1 female, which we then restrict to females using a gender filter.
- **Campaign 2:** We create a Custom Audience which included 4 people that lived at the same known address. We then added a geo-fencing that restricted the campaign to a 1 mile radius around that address.
- **Campaign 3:** We used inclusion/exclusion features to geo-fence an apartment building and target people living there. We did not use custom audiences.

We created a Facebook page and linked it to a Business Ad account, from which we ran both campaigns. We used ads that we created specifically for the study, as shown in Fig. 2. We designed it so it could be easily noticeable while gently reminding the ad was displayed for experimental purposes. We ran Facebook ads in the month of March and April 2019.

Participant Recruitment: In order to create a *Custom Audience*, a list of personally identifiable information corresponding to the Facebook accounts of at least 20 people is required. To collect that data, we sent out a survey [52] that asked for email address, name, gender, date of birth, city of residence and consent for us to use this data in the context of our investigation. The survey was first sent to friends and relative, and we encouraged them to share it along. We collected 38 responses in total, with 26 men and 12 female (self-identified) ranging between 18-34 years old, living in the US and India.

Figure 2: Facebook ad copy used in the campaigns

Table 1: Comparison of Attack Vectors

Criteria	**Strategy 1**	**Strategy 2**	**Strategy 3**
Core audience	26 male, 1 female	26 male, 12 female	anyone
Target Gender	Female	All	All
Location	United States	specific address (1 mile radius)	specific address+location exclusion
Placements	Automated	Automated	Automated
Campaign goal	Maximize Impressions	Maximize Impressions	Maximize Impressions
Interests	Not applicable	Not applicable	Not applicable
Devices	All	All	All
Snipping successful?	**No**	**Yes (partially)**	**No**

Analysis Methods: To track the impressions of our campaigns, we mostly relied on Facebook Ads Manager. The tool gives a unified dashboard with the number of impressions and other key metrics, for all the campaigns associated with the account. We asked our participants to report to us whenever they saw the test ad, so we could match these views with the impressions monitored in Facebook Ads Manager.

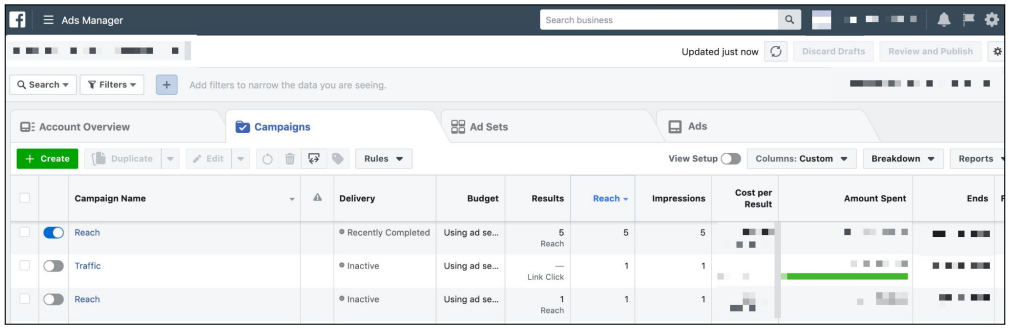


Figure 3: Facebook Ads Manager shows the reach and impressions for each campaign

6.1.3 Results

Finding 1 - Facebook Custom Audiences can be combined with geo-targeting to perform sniper-targeting

We were able to target an individual using the Campaign Strategy 2. We can confirm that at least one out of the four individuals, living at the specific address we targeted, saw our advertisement. Facebook's ads manager reported a total of 5 impressions on Instagram.

Figure 4: Audience insights for the geolocation targeting campaign

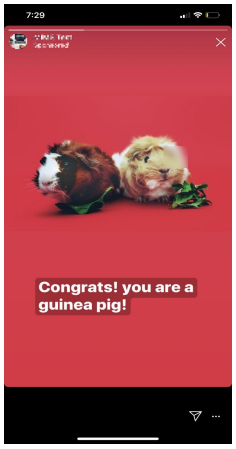


Figure 5: Here is the ad impression on Instagram stories using the geo-location strategy

The one confirmed ad impression was in the Stories section of Instagram, shown in Fig. 5. We were unable to determine who saw the 4 other impressions that Facebook ads manager reported. We suspect it was someone from our audience who may not have scrolled past the ad without paying attention to it.

As illustrated on the Fig. 6, the audience definition grows if we change the targeting from gender based to location based. Our hypothesis is that when we used location targeting on top of the custom audience, Facebook believed the audience definition was wide enough to serve ads. But in reality, we were trying to target the 3-4 people who we knew lived at the address who were also in our custom audience.

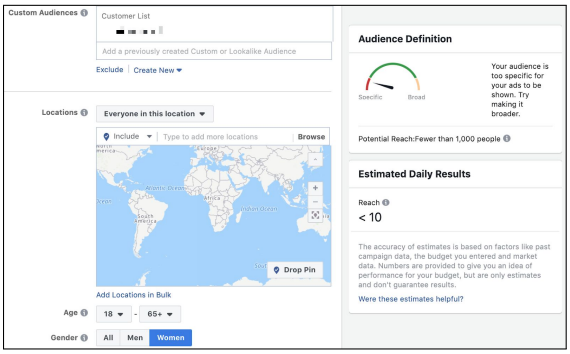
Our interpretation is that since we choose the "everyone in this location" targeting criteria, Facebook was unable to deterministically know that the audience definition was less than 20. It may be using some statistical estimate of how many people from the audience might be at that location. This estimate may have been greater than 20.

In Campaign Strategy 1, we used an audience with 27 male and 1 female and added gender based targeting on top to target females. Theoretically, if an ad was served it would have been to the 1 female member of this audience. But, since in this scenario, Facebook did not serve ads since it deterministically knows that the audience is less than 20.

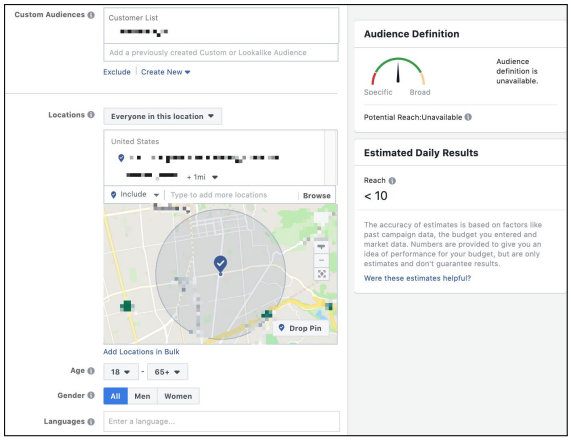
This changed in Campaign Strategy 2. As seen on Fig. 6, the audience definition grows if we changed the targeting to from gender based to location based (within 1 mile radius of a specific address). This allowed us to target people who are in that zone. We ran additional campaigns using the Campaign Strategy 2. As shown in Fig. 3, we got 1 impression in each but we don't know who saw it since the impressions were no self-reported by our subjects.

In Campaign Strategy 3, we did not use a custom audience but geo-fenced a specific address to get the target zone to an area of a few square meters (see Fig. 7). We see in this case (see Fig. 7) that the audience definition is too specific if we only target 'people living in this area'.

When we used 'Everyone in this location', the audience definition increase and we were able to get impressions from many users. We notice that this vulnerability (reported before by [37]) can still be used for micro-targeting, but is not a precise sniper-targeting method. In less populated areas, it might be more efficient.

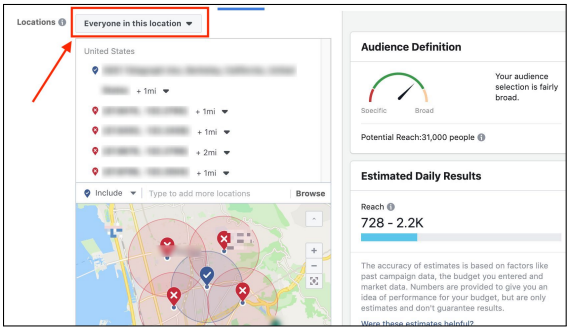


(a) Gender Targeting

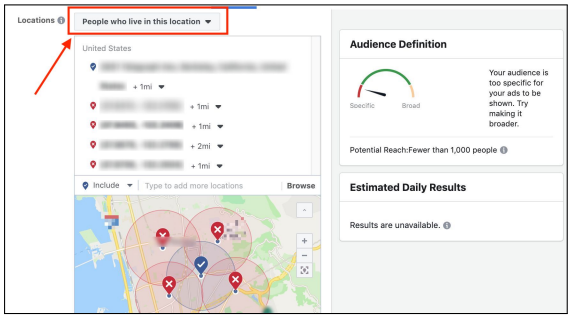


(b) Location Targeting

Figure 6: Audience definition broadens when using location based targeting



(a) Geo-fencing: Everyone in that location



(b) Geo-fencing: People living in that location

Figure 7: Audience definition is too specific when we geo-fence people living at a particular address

Finding 2 - The minimum audience size is not large enough to deter sniper targeting.

Facebook warned us that the audience for Campaign Strategy 1 was too narrow for the ads to be shown. It was true. We were not able to any get ad impressions for Campaign Strategy 1. The strategy in the Medium article [8]

that we were trying to emulate was written in Dec 2017 and we believe that Facebook has updated their workflow since. Now do not allow the audience definition to be less than 20 people. This may also be as a consequence maybe as a consequence of [37].

We should call out that Facebook doesn't explicitly state 20 as the minimum audience size but in our research we found several posts online which stated that they 20 was the minimum permissible audience size [53].

This size is meant to protect against individual targeting but anyone with the motivation and a little bit of resources can find (or create) 19 accounts to collude with and add them to the audience along with the 1 account that this person really wants to target/influence. This loophole has also been identified in other studies as well [37].

Finding 3 - Custom audience data sources are not verified.

Facebook does not verify where the data actually came from. However, it does ask the user to self attest to the original source of the data through a drop-down list. Options are:

- **From customers and partners.** Advertisers collected information directly from their customers and it was also sourced from their partners (i.e. agencies).
- **Directly from customers.** Advertisers collected information directly from their customers.
- **From partners.** Advertisers collected information directly from their customers and it was also sourced from their partners (i.e. agencies).

Facebook does the identity matching on a variety of indicators to match users such as name, phone number, email ID, gender, age, location/address to name a few. So in theory, anyone who has your personal information (which you linked to Facebook) can add you to a custom audience without seeking your approval.

Finding 4 - Some spillover must be tolerated.

Targeting just a single person on Facebook is challenging. Geo-fencing cannot guarantee that only the person you want to target will see ads. In Campaign Strategy 2, anyone in the attack location who was part of our custom audience could potentially have seen the advertisement, even if they were just passing by that location. See table 1.

We ran multiple campaigns with a similar strategy but were unable to determine if we consistently reached our target since we were reliant on self-reported data to match the reach/impression numbers we saw on Facebook Ads Manager.

Some spillover must be acceptable when trying to reach someone with this method.

6.1.4 Limitations

Reporting: We were only able to confirm that our ads were reaching the intended set of people through self reported data. For the ad campaign that used the location based strategy, Facebook ads manager reported 5 impressions but we could confirm only 1 of those impressions to be actually seen by a study participant and reported back.

Viewability: This ties into the reporting limitation talked about in the previous paragraph. Ad viewability can also be a limitation of our study. Viewability standards defined by the IAB and if an ad meets those standards then Facebook will count it as a viewable impression. This however does not mean that the viewer's brain actually registered the ad. Humans have learned how to ignore ads when they are browsing their favorite social media apps or browsing the web. Thus, an impression registered on Facebook does not always mean that the viewer can recall seeing the ad.

Reproducing Results: We do not have inside access to Facebook's systems and employees. Thus, at this point we can only state the results and propose our hypothesis as to why we did or did not get the results we expected. Only Facebook can truly explain why certain things worked and others did not. Additionally, we ran the location targeting campaign multiple times over the course of our study but not all campaigns delivered impressions.

6.2 The Spinner

6.2.1 Context

Until very recently, reported instances of sniper-targeting had been performed by online advertisement experts, who were savvy enough to exploit the platform. Recently a service appeared in the news [39, 54, 15] allegedly offering a seamless sniper-targeting service for everyone to use. Founded in April of 2018, the site claims to help customers target loved ones or acquaintances to subliminally influence them to change their behaviors through being repeatedly shown manipulative ads disguised as editorial content. The website reports a user base of 140,000 people, although there are no reason to believe that this number is accurate.

According to this site, for the price of $29.00, the targeted individual will be shown "approximately 10 articles, 180 times, over three months." The purchaser can choose from existing campaigns, ranging from health (stop smoking, quit drinking) to economic (settle a divorce, buy a dog) to behavioral (initiate sex, become a vegetarian), or request for a custom campaign. Due to privacy laws, the service is not allowed for Europeans, to either purchase or to be targeted.

Despite the service banning European IPs from accessing the site, Eliott Shafler, co-founder of The Spinner's and head of marketing and social, argues that they are breaking no laws and that their purpose is to allow everyone, not just the big companies, access to using advertising to manipulate others:

> *"The Spinner is only different because it's an average person targeting another person. All you need is your phone and a few dollars and you can have a targeted PR campaign. If you're freaked out by The Spinner, you should be freaked out also by all the brands."* [39]

Nonetheless, the company intentionally conceals all information about the company. The servers are registered with the WHOIS Privacy Service, an option used to keep the registrant identity private. No information about the identity of the two founders is found online, and they refuse to be photographed or to name their university affiliation. [rolling stone] The company is allegedly registered in London [39], but their website states that *the Terms, the Software and the Service will be governed solely by the laws of the city of St. Petersburg, Russia*. This incoherence raised the suspicion of a journalist investigator, who linked the site to an Israeli company and investor.[55] This blatant opacity casts doubt as to whether the founders of the Spinner truly believe that their service abides by the law, and weather the service actually achieves what it claims to do.

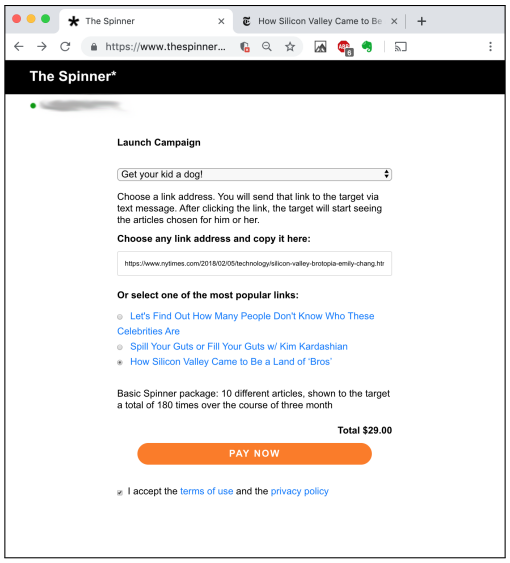
Several journalists have in fact conducted their own experiments with The Spinner [56, 3, 15, 54], finding that the targets were served multiple campaigns and that targets did not generally notice anything strange with their ad experiences during the period [56]. According to them, articles would appear through ad distributors such as Revcontent, Outbrain, Exoclick, and Facebook. A few did not ever see the ads they tried to target themselves with [3]. Some wonder at its effectiveness and if it is actually a scam [56, 3].

6.2.2 Study Design

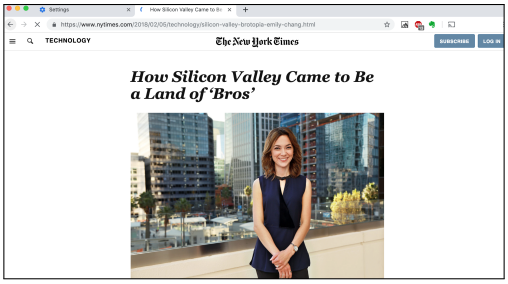
Research Goal: We explore the effectiveness of the service, by tracking the ads received by an individual who consented to be targeted by campaign. We analyze how the cookie Spinner cookie interferes with the ad network to deliver ads.

Implementation: We bought a campaign on March 18, 2019 for The Spinner campaign for "Get Your Kid A Dog!", shown in Fig. 8a. The user is asked to pick an innocuous link with which to send to their target. The associated link we chose goes to an article titled "How Silicon Valley came to be the Land of the Bros" as shown in Fig. 8b

After purchase, two targets were given the link and asked to click on it. The control is the real target and is supposed to click on the link as if just sent from a trusted friend. The second target will attempt to open the link using countermeasures such as incognito mode, ad blockers, and cookie deletion. The control will employ no such countermeasures, opening the link in a normal window with no ad blockers or other such plug-ins.



(a) Setting up a The Spinner campaign.



(b) Chosen web link associated with campaign.

Figure 8: Initial Setup for The Spinner campaign

The control target will be asked to keep a diary journal over the course of 90 days, the full length of the campaign. They will be shown the target ad to expect and all other potential campaigns served by The Spinner. If they see any ads belonging to any Spinner campaigns, they are requested to take a screen shot of the ad and a sample of ads directly before or after its placement. We also asked them to record the time of the event and site they were on. Lastly, we asked them to write a few sentences about anything the notice and how they felt about the experience.

Initially, the control target was asked to not interact with the ads if shown. Halfway through the targeting, we asked the control target to click on one of the links.

Technical investigations was conducted on both the control and countermeasure targets' desktop devices: looking at the browser conditions of the heap and cookies.

Participant Recruitment: Two individuals were targeted in this study: one researcher and one non-researcher participant. The non-researcher participant was the control target and was recruited by convenience. Criteria for selection included existing social media usage, frequency use of internet, lack of ad blockers, willingness to share their ad experience over a period of several months, and willingness to allow researchers access to their devices on which ads were served. One researcher was also targeted while taking countermeasures to analyze effective ways of avoiding this method of targeting.

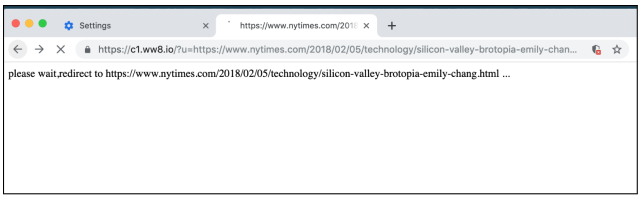
6.2.3 Results

Finding 1 - The Spinner does not serve the ads that have been paid for.

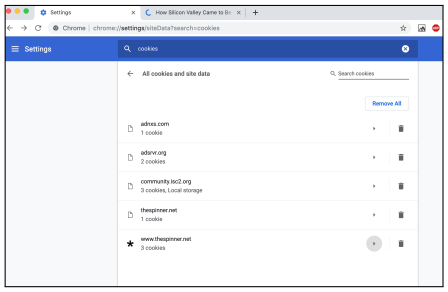
The link is a short URL that appeared to be from Google. When clicked it goes to a redirect (shown in Fig. 9a), at this point several cookies are downloaded to the browser (shown in Fig. 9b and Fig. 9c).

The control target, after clicking on the link once, immediately saw ads on their Facebook feed on their desktop device and shortly after on their mobile Facebook app as well. The link was clicked on while on their desktop device. The first ad they saw is shown in Fig.

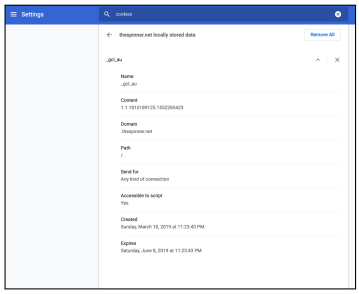
For the first month, we asked them not to interact with the ads in any way. Only to record what they experienced. During this time they reported seeing a relevant ad about once a day, usually within the first five minutes of going



(a) Redirect page after clicking on what appears to be a Google shortened link.



(b) All cookies in browser memory after clicking on short URL (all cookies had previously been deleted).



(c) Inner contents of one of the Spinner specific cookies.

Figure 9: Redirect landing page for The Spinner saves several cookies to the browser.

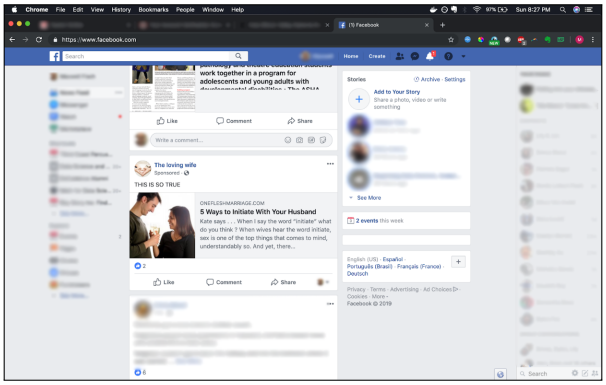


Figure 10: First ad seen by control target.

on Facebook. Ads could appear either in their main feed or on the sidebar. No ads were seen in any non-Facebook environments. In the second month, we asked the control target to click on one ad, after which they saw a few of the same ad while browsing the web served via Outbrain.

Our results corroborated several of the experiences of the journalists. The control target never saw the actual bought campaign, regarding buying a dog, instead reporting seeing mostly both ads asking them to "initiate sex with their husband" as well as "propose to their girlfriend."

Finding 2 - Not clicking on links limits targeted advertising

The Spinner method is essentially a combination of spearphishing[1], using an URL redirect that leaves cook-

[1]Spear phishing is a personalized email or electronic communications that attempts to lure the target into sharing sensitive information. The most common vector for attack is to send an email to the target inviting them to click on a malicious link. In this case, this would be the email we sent to the control target with the redirect link which took them to a site that downloaded several cookies to their browser.

ies, enabling the site to then pool individuals into a more traditional advertising campaign model of utilizing previous behaviors (clicking on a cookie loaded link) to select for further advertisements. If the user deigns to click on the targeted advertisement, this in turn generates more cookies, which is then used to follow them elsewhere on the web[2], e.g. denoting to advertising services such as Outbrain that they should be shown an ad because they have previously clicked on something related to it.

In our study, we asked our control target not to interact with the ads in any way for the first month. During that time no ads on any platform other than Facebook was served. Later we asked them to click on one link. Soon afterwards, they saw two Outbrain sponsored ads in the same day, but none afterwards. While our targets will in no way reach the purported metric of 180 times over 90 days or observed the ads following them all around the web, one could imagine that this method can easily snowball into a large number of impressions if the user was less fastidious about not clicking on links.

Finding 3 - Regular browser hygiene can prevent The Spinner method

Analysis from the countermeasure target found that the following methods prevented this form of ad targeting:

- Adblock browser plugin while clicking on the link
- Deleting cookies (immediately after clicking the link and before going to Facebook)
- Disabling (on Chrome) the setting of "Allow sites to save and read cookie data" - however it is worth noting that doing so will cause many sites to stop working or refuse access including Facebook

While the following method did not prevent targeting:

- Browsing in Incognito Mode - this does not save cookies between sessions, however does nothing to limit their usage within session
- Adblock browser plugin turned on after having clicked on the link with it turned off

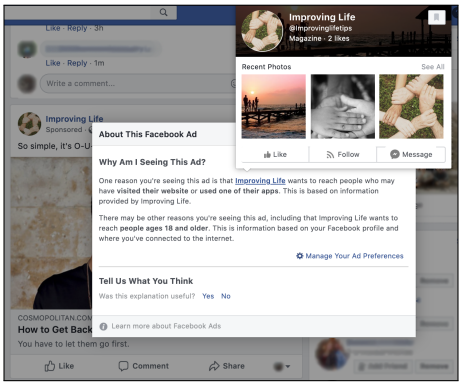


Figure 11: Utilizing Facebook feature of "See why am I seeing this ad" on Spinner based ad. We find that The Spinner has created several lifestyle oriented Pages. The retargeting works by using a cookie that indicates to Facebook that the target user has recently visited a site associated with one of The Spinner's lifestyle Pages.

These findings indicate that the technical process for how The Spinner works is that the Google shortened link actually goes to a dummy page that immediately redirects to the article. While on this dummy page (shown in Fig. 9a) a batch of cookies are saved to the browser (shown in Fig. 9b). Utilizing Facebook feature of "See why am I seeing this ad"

[2]This is considered re-targeting, which is serving ads to potential customers based on cookies on their browser, usually cookies that indicate they have previously been to the advertiser's site.

(shown in Fig. 11, we can see that Facebook shows these ads because they believe The Spinner associated campaign has indicated that the user has previously been to one of their sites. Thus we can deduce that one of the loaded cookies indicates that the target has been to a site associated with the campaign and thus shown interest in the content of the ad campaign.

While The Spinner allows the targeting of individuals, they are not doing this action through individual targeting, but rather by associating individuals with ongoing campaigns. This explains our experience and previous reports of targeted individuals getting a wider spread of The Spinner campaign advertisements and even not getting the ad they actually signed up for.

Finding 4 - User experienced normalization of advertised content within days

The control target recorded 74 ads in the diary journal over the course of 90 days; 72 on Facebook divided between desktop and mobile, 2 on a news article that they were directed to after clicking a link from within Facebook. They found that the ad that they did not really notice ads that pertained to them. It was ads that they felt had nothing to do with them, e.g. "Stop smoking," that stood out. More concerning was how quickly the ads became the new norm for them: "the advertisements went from being humorous to insidious to normalized over the course of days. By day 3 or 4 it was just the new normal. If I had a husband, I would have thought initiating with my husband was just something a lot of people thought about now."

Despite their dismissal at the advertising's effectiveness at behavioral change, the target user felt that the tool was effective for altering what people thought was normal, making it a tool ripe for harassment and cyber-bullying or to sway powerful individuals such as politicians. They were concerned with how easy it was to become a target and could see it as being very effective; finding it concerning that someone could have that much"individual power" to change the sense of what is normal for another individual person. The user stated that the normalization made it easier to think about the content of the ads, talk about it in real life, and in general just feel that those contents were things that were just said online and offline or that one should see in their online environment. They remained unconvinced the advertising would lead to action.

The advertising may not make you directly more likely to do something, but it would make you think it was normal to see or talk about it. Perhaps more concerning from the user feedback is that, while knowing they were being targeted and asked to record it, they felt they got used to the targeted ads fairly quickly and that it became a normalized part of their existing ad experience. This suggests that even when users are actively made aware there is a strong tendency to normalize both the contents and behaviors of advertising.

6.2.4 Limitations

For the purposes of this experiment, we needed real users with real browsing activity thus it was difficult to thoroughly investigate the cookies as maintaining an environment free of other cookies was essentially impossible. Since advertising does depend upon the existing behaviors and attributes known about the user, it is possible that we may have had different results with a different person as the control target. Our target did not actually experience an ad that followed them around the web, but rather a daily exposure on one social media platform and we should consider that the behavioral outcome may change depending on the frequency and spread of the ad exposure. Lastly, our test was for a campaign that cost less than thirty dollars for around three months of somewhat daily exposure. Real world target sniping cases with real budgets could easily achieve much higher levels of exposure to consistent materials.

6.3 Other Investigations

6.3.1 Google Adwords

We tried to test if sniper-targeting could be acheived using Google Adwords, combining geo-fencing with keywords that are only likely to be searched by specific individuals.

Upon registration, Google restricts the account to Adwords Express, which has restricted targeting feature as compared to the full version of AdWords. We tried contacting the customer service, but got no response, probably because our the ad budget was too small.

We then tried to run a sniper targeted ad from Adwords express, restricting the geographic are to Berkeley, CA using a personal address as keyword. The idea is that the resident of that house in much more likely that anyone else to google their own address, for instance to look up the directions. We also tried using a first and lastname as keywork, based on a similar assumption.

We were unable to see these ads. It is unclear if this is due to the limited affordances of AdWords Express, which only allows to target on similar expressions but not on explicit keywords or if Google has safeguard in place to prevent such exploits. We were able to sniper-target ourselves from that same interface using a french onomatopoeia keyword 'ouais'. A few weeks after we contacted Google's customer service from the account that was used for the experiment, the AdWords account was shutdown.

The experiment did not allow us to draw clear conclusions, but it seems that Google is more wary than Facebook about potential misuse of their ad platform. It is nonetheless possible to envision sniper-targeting attacks on Google Adwords, even without using personally identifiable information as keywords. For instance the didgeridoo player from a small town described in [section 4.2] could be sniper-targeted with arbitrary ads by combining geo-fencing and the 'didgeridoo ' keyword.

6.3.2 Malicious Browser Extensions

The term *Ambient Tactical Deception* was introduced in the 2018 Trowbridge paper to describe the use of a malware to perform 'Internet-based manipulation of an individual or group reality' [57]. This strategy can be exploited to perform sniper-targeting, by having a target install a malicious browser extension which would discreetly alter the ads that are being displayed.

A variety of mal-wares could be thought of along these lines, and it would not be surprising to see this sort of attack become increasingly popular in the context of the information warfare described in part 3.2.

7 Recommendations

7.1 For Users

Opt-outs:
As seen in Fig. 12, Facebook does allow their users to see which advertisers have added them recently to a customer list and target ads and opt out of ads from any of them. But the list contains hundreds of advertisers and it seems unlikely that the average user will ever look at them.

Additionally, users can prevent ads personalization based on their activity on Facebook products or other websites (see Fig. 13).

Adblock and Deleting cookies:
As previously mentioned in results for The Spinner method (Section 6.2.3), users can use adblock browser plugins that limit javascript from running, which can drastically decrease the pervasiveness of cookies. Regularly purging cookies can also be useful, however comes with the burden that doing so will automatically log the user out of almost all accounts. Perhaps more important is for users to understand that Incognito Mode is not a panacea for web browsing safety and will not actually make them free from tracking or detection. If you are sent a link or directed to go to an unknown website, using Incognito Mode does not prevent cookies from being saved to your browser.

Figure 12: Users can see which advertisers have added them to an audience on Facebook (blurred intentionally)

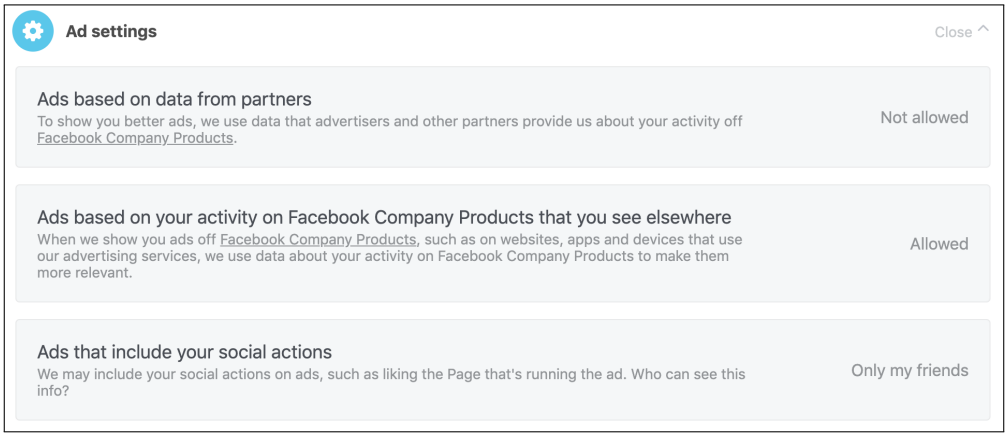


Figure 13: Users can opt-out of ads personalization based on their activity on or off Facebook

7.2 For Policymakers

In our limited targeted advertising experiment, we found that the user, while knowing what content to watch for, experienced a shift in their perception of what was normal along with normalization of the advertising method. While targeted advertising may not be subliminal messaging per se, we should consider the 1974 FCC policy advice against the use of "subliminal perception" and as "contrary to the public interest" [46]. Targeted advertising could be used to sway key individuals or via advertising personalized to single individuals at scale in order to shift public norms without discourse, awareness, or opportunity for redress and sold piecemeal to anyone with the funds.

The current infrastructure of the internet, such as cookies and the asynchronous web, allows for the proliferation of technology that will continue to enable target sniping. We have explored two means of target sniping via our technical investigation: ad bidding using target data and re-targeting via cookie based spear phishing. At its core, both rely on the internet infrastructure's capacity to collect information about us or serve information to us across our sessions of

internet activities. The economic motives of the dominant ecosystem of the internet will continue to be based upon ad revenue and the infrastructure will be unwilling and slow to change in ways that inhibit advertising targeting activities.

Currently, Facebook uses an opaque mechanism of bidding strategies, ad relevance ranking and likelihood of a click to select which ads will be shown to the user. Policymakers could compel Facebook to be more transparent about the rules they are applying to decide whether a campaign's ads are served or not served, and force changes to these rules if they remain to easily exploitable.

For policy makers and advocates, there are a few key recommendations to consider:

- Validate. Collaborate with technical experts to continually validate that "fixes" have actually been implemented.
- Stay vigilant. The advertised privacy situation may not correlate with the implemented reality. Historically, privacy has been oversold and needed fixes delayed.
- Assume the lack of privacy unless proven otherwise. Understand that the current infrastructure and economic incentives inherently works against privacy.
- Ask for transparency that can inform. It is difficult to make decisions on what we do not know. While platforms have made improvement (e.g. Facebook's "See why am I seeing this ad" feature), we need to take steps towards transparency that can enable the everyone to make informed decisions.
- Consider the entire technical ecosystem. Desired policy outcomes may not be deliverable under the current infrastructure paradigm: e.g. trying to serve privacy at the endpoints and leaving the ISPs out of the equation may not be a tenable approach to long-term privacy.

7.3 For the Digital Ad Industry

Increase the minimum audience size:
The minimum audience size (post ID matching) that are allowed to be created could be increased so as to deter individual targeting. Facebook needs to find a balance between user privacy and ad platform effectiveness such that its bread-n-butter micro-targeting would still be possible.

Adopt a multi-tier model of feature access:
Rather than allowing anyone to wield the power of the full set of targeting features available, Facebook could vet ad accounts and only then offer full feature suite access. Unvetted advertisers could have blunter targeting tools which may prevent misuse and sniper targeting. Our experiment on AdWords [part X] suggests that Google may be using a strategy along those lines.

8 Conclusion

The ability to target arbitrary users with individually-tailored ads at relatively low cost brings about new risks of manipulation, cyber-attacks and information leaks.

Despite having been publicly documented for almost a decade, sniper-targeting vulnerabilities on major ad platforms have received little attention. Recently, the phenomenon was featured in several media as a shady company offered to make this exploit available to regular end-users.

Our investigation shows that the capabilities of this service are overstated and are actually quite limited. Nonetheless, several trends lead us to be wary that such tools might become increasingly effective and prevalent in the near-future:

- Generalized tracking and monitoring of internet users keeps intensifying, and the convergence of data sources into unified databases makes it increasingly easy to match cookies and other digital trackers with an individual's identity [4].

- The intensification of computational propaganda and manipulation efforts around the world and the diversification of actors taking part in information warfare will drive up the demand for sniper-targeting tools [28].
- The digital advertising industry is reluctant to address the problem since the technical solutions which could limit sniper-targeting tend to restrict micro-targeting possibilities.

Facebook's attitude on this issue confirms this last point. The company received several alerts regarding its vulnerability to sniper-targeting attacks, to which they either failed to respond or responded with minimal and partially ineffective fixes in order not to impact their business interests [2, 37, 58].

Given these adverse financial incentives, sniper-targeting would need to be restricted by regulators in order to be contained but current legal frameworks in the US do not clearly outlaw the practice. Considering the many risks for end users which this practice entails, it is urgent to act.

References

[1] Facebook. About custom audiences. https://www.facebook.com/business/help/744354708981227.

[2] Aleksandra Korolova. Privacy Violations Using Microtargeted Ads: A Case Study. page 24.

[3] Kevin Poulsen. For $29, You Can 'Brainwash' Someone on Facebook. January 2019.

[4] Anthony Nadler, Matthew Crain, and Joan Donovan. The Political Perils of Online Ad Tech. page 47.

[5] How I Pranked My Roommate With Eerily Targeted Facebook Ads, September 2014.

[6] Jules Schroeder. The Magic Formula Behind Going Viral On Reddit.

[7] Direct Marketing and Nanotargeting | MIT Social Media Hub.

[8] Michael Harf. Sniper targeting on facebook: How to target one specific person with super targeted ads. https://medium.com/@MichaelH_3009/sniper-targeting-on-facebook-how-to-target-one-specific-person-with-super-targeted-ads-515ba6e068f

[9] Facebook Ads Sniper Method: How to Put Your Ad in front of ONE Specific Person — Jonathan Hawkins.

[10] Caroline Haskins. Facebook ad micro-targeting can manipulate individual politicians.

[11] Tim Shipman Political Editor. Labour HQ used Facebook ads to deceive Jeremy Corbyn. *The Sunday Times*, July 2018.

[12] John Oliver wants to educate Trump, so he bought ads on Sean Hannity's show.

[13] CBS. The good fight tv show. https://www.youtube.com/watch?v=sgyIQDBL0KQ&t=1s.

[14] Inside the Secret Facebook War For Mormon Hearts and Minds.

[15] Simon Chandler. Facebook is helping husbands 'brainwash' their wives with targeted ads. *The Daily Dot*, 2019. https://www.dailydot.com/debug/husband-brainwash-wife-spinner-ads-facebook/.

[16] How does it benefit me? | NAI: Network Advertising Initiative.

[17] Our Senate testimony on online advertising and Google-DoubleClick.

[18] Led Astray: Online Lead Generation and Payday Loans.

[19] Salud America! Rudd Center for Food Policy Obesity, Council on Black Health. Increasing disparities in unhealthy food advertising targeted to hispanic and black youth.

[20] ACLU and Workers Take On Facebook for Gender Discrimination in Job Ads.

[21] HUD.gov / U.S. Department of Housing and Urban Development (HUD).

[22] Facebook Settles Civil Rights Cases by Making Sweeping Changes to Its Online Ad Platform.

[23] Doing More to Protect Against Discrimination in Housing, Employment and Credit Advertising | Facebook Newsroom.

[24] Till Speicher, Muhammad Ali, Giridhari Venkatadri, Filipe Nunes Ribeiro, George Arvanitakis, Fabrício Benevenuto, Krishna P Gummadi, Patrick Loiseau, and Alan Mislove. Potential for Discrimination in Online Targeted Advertising. page 15.

[25] Tega Brain. The New Organs.

[26] Elleen Pan, Jingjing Ren, Martina Lindorfer, Christo Wilson, and David Choffnes. Panoptispy: Characterizing Audio and Video Exfiltration from Android Applications. *Proceedings on Privacy Enhancing Technologies*, 2018(4):33–50, October 2018.

[27] PWC. Iab internet advertising revenue report.

[28] Samuel C. Woolley and Philip N. Howard. *Computational Propaganda*. Oxford Studies in Digital Politics. November 2018.

[29] Josh Nathan-Kazis Justin Elliott. D.C.-Based Pro-Israel Group Secretly Ran Misleading Facebook Ads to Target Pro-Palestinian Activist, September 2018.

[30] Al Jazeera. Watch the film the Israel lobby didn't want you to see, November 2018.

[31] Opinion | We Made A Documentary Exposing The 'Israel Lobby.' Why Hasn't It Run?

[32] Tasmin Shaw. *Invisible Manipulators of Your Mind*.

[33] P. H. D. Media. New Beauty Study Reveals Days, Times And Occasions When U.S. Women Feel Least Attractive.

[34] S. C. Matz, M. Kosinski, G. Nave, and D. J. Stillwell. Psychological targeting as an effective approach to digital mass persuasion. *Proceedings of the National Academy of Sciences*, 114(48):12714–12719, November 2017.

[35] Segment-of-One Marketing.

[36] Jennifer King. Privacy, Disclosure, and Social Exchange Theory. page 207.

[37] Irfan Faizullabhoy and Aleksandra Korolova. Facebook's advertising platform: New attack vectors and the need for interventions. *arXiv:1803.10099*, 2018.

[38] Athanasios Andreou, Marcio Silva, Fabrício Benevenuto, Oana Goga, Patrick Loiseau, and Alan Mislove. Measuring the Facebook Advertising Ecosystem. page 16.

[39] Lou Stoppard. Inside the spinner: a real-life inception project. *Financial Times*, 2018. https://www.ft.com/content/944d068c-8a99-11e8-affd-da9960227309.

[40] Olivia Goodkin Maureen Ann Phillips. The subconscious taken captive: A social, ethical, and legal analysis of subliminal communication technology. *S. CAL. L. REV.*, pages 1077, 1079–80, 1981).

[41] Susan Akbarpour. How does gdpr impact advertising and e-commerce? *Forbes Magazine*, 2018. https://www.forbes.com/sites/forbesagencycouncil/2018/05/08/how-does-gdpr-impact-advertising-and-e-commerce/#86f366c32776.

[42] Steven Melendez. How google is breaking eu privacy law, according to a new complaint. *Fast Company*, 2018. https://www.fastcompany.com/90236273/google-faces-gdpr-privacy-complaint-over-its-targeted-ads-from-brave-browser.

[43] Chris Shuptrine. Gdpr and ad tech: The definitive guide of 2019. *Adzerk*, 2019. https://adzerk.com/blog/gdpr-ad-tech/.

[44] John J. Heitmann. Will your tv watch you? fcc green lights targeted advertising in next gen tv broadcasting standard. *CommLaw Monitor*, 2019. https://www.commlawmonitor.com/2017/11/articles/privacy/will-your-tv-watch-you-fcc-green-lights-targeted-advertising-in-next-gen-tv-broadcasting-standard/

[45] Brian Fung. Tv stations are about to track you and sell targeted ads, just like google and facebook." tv stations are about to track you and sell targeted ads, just like google and faceboo. *Los Angeles Times*, 2017. https://www.latimes.com/business/technology/la-fi-tn-next-gen-tv-20171114-story.html.

[46] Harold Furchtgott-Roth. 9/19/00 speech by commissioner harold furchtgott-roth: The fcc's investigation of "subliminal techniques. 2000. https://transition.fcc.gov/Speeches/Furchtgott_Roth/2000/sphfr011.html.

[47] Lynne Chandler Garcia and John R. Vile. Abortion protests. *THE FIRST AMENDMENT ENCYCLOPEDIA*, 2017. https://www.mtsu.edu/first-amendment/article/13/abortion-protests.

[48] Nina Totenberg. Should polling places remain politics-free? justices incredulous at both sides. *NPR*, 2018. https://www.npr.org/2018/02/28/584606124/polling-place-battleground-freedom-of-speech-versus-freedom-from-intimidation.

[49] Markets and advertisers rush to comply with california privacy law. *Morning Consult*, 2018. https://morningconsult.com/2018/12/18/fresh-off-gdpr-companies-now-have-to-prepare-for-californias-privacy-lawl.

[50] Giridhari Venkatadri, Athanasios Andreou, Yabing Liu, Alan Mislove, Krishna P. Gummadi, Patrick Loiseau, and Oana Goga. Privacy Risks with Facebook's PII-Based Targeting: Auditing a Data Broker's Advertising Interface. In *2018 IEEE Symposium on Security and Privacy (SP)*, pages 89–107, San Francisco, CA, May 2018. IEEE.

[51] Facebook. Data types allowed. `https://www.facebook.com/business/help/606443329504150?helpref=faq_content`.

[52] Sniper targeting survey. `https://berkeley.qualtrics.com/jfe/form/SV_3kM53EJ2KLU5sXj`.

[53] Quora. Quora question. `https://www.quora.com/What-is-the-minimum-audience-size-number-for-Facebook-ads`.

[54] Parmy Olson. For $29, this man will help manipulate your loved ones with targeted facebook and browser links. *Forbes*, 2019. `https://www.forbes.com/sites/parmyolson/2019/01/15/a-shadowy-entrepreneur-claims-his-online-manipulation-business-is-thriving/#69a2bbe072a9`.

[55] Nexter Dror Bloberman. House of Lies, September 2018.

[56] Tracy Moore. I tried to brainwash my coworker with a sketchy facebook ad campaign. *MEL Magazine*, 2019. `https:/melmagazine.com/en-us/story/facebook-spinner-ad-manipulation`.

[57] Adam Trowbridge, Jessica Westbrook, and Filipo Sharevski. Sorry: Ambient Tactical Deception Via Malware-Based Social Engineering. *arXiv:1810.11063 [cs]*, October 2018. arXiv: 1810.11063.

[58] Bryan Carney. Sneaky 'Sniper-Targeting': Tyee Proves Facebook Privacy Flaw Still Exists, April 2019.

Glossary

cookies Cookies or HTTP cookies are small pieces of code that can be generated when an user interacts with websites. These code gets added to the user's web browser and is stored on the computer over a set period of time by the developers or until deleted by the user. They are used by websites to remember information about the browsing state of the user to enable better performance. For instance, it allows to keep track of a shopping cart on a web-store even without signing-in, including across tabs and sessions. Due to their ability to recording and retain web activity information, cookies can also be used to record the user's browsing activity or follow the user across sites on the Internet; like a trail of crumbs, enabling sites to know where the user has been and what they have been doing.. 16–19

custom audience A custom audience from a customer list is a type of audience you can create made up of your existing customers. You can target ads to the audience you've created on Facebook, Instagram, and Audience Network. 12, 14

impressions The number of times the ad was seen. 11–14

reach The number of people who saw your ads at least once. Reach is different from impressions, which may include multiple views of your ads by the same people. This metric is estimated. 14

viewable impression A viewable impression is a standard measure of ad viewability defined by the International Advertising Bureau (IAB) to be an ad which appears at least 50percent on screen for more than one second. Viewable impressions are the metric that advertisers use to quantify the percentage of ads that are actually viewed by real people. 14