Venture: The University of Mississippi Undergraduate Research Journal

Volume 6 Article 7

10-2-2024

Targeted Advertising: How Companies And Governments Are Weaponizing User Data Against The Consumer

Joseph Garneau
University of Mississippi

Recommended Citation
Garneau, Joseph (2024) "Targeted Advertising: How Companies And Governments Are Weaponizing User Data Against The Consumer," *Venture: The University of Mississippi Undergraduate Research Journal*: Vol. 6, Article 7.
Available at: https://egrove.olemiss.edu/umurjournal/vol6/iss1/7

Targeted Advertising: How Companies And Governments Are Weaponizing User Data Against The Consumer

Joseph Garneau

ABSTRACT

With the recent rise of a new digital age, many people are ditching more traditional methods of performing everyday tasks and replacing them with free and convenient online services. But as the saying goes, there is no such thing as a free lunch, and that sentiment holds true in terms of online services as well. Consumers pay for these online services with something much more valuable than money—their personal data. This paper explores how companies and governments present consumers with targeted advertisements, shows how targeted advertisements are inherently manipulative, and gives an example of one government and one company using this technology to influence the behavior of its target demographics. The paper concludes with a discussion of the ethical implications of the research, states its limitations, proposes possible solutions by providing contextual information, and concludes by arguing that the only way to change this behavior would be through legislative measures.

Introduction

After the unfortunate passing of Linday Robertson's mother in 2014, she took on the responsibility of arranging her mother's affairs (Nudson, 2020). One of those responsibilities was to figure out a price for a gravestone, and, after a quick Google search, Robertson soon found what she was looking for and ended her browsing session. However, like a restless soul with unfinished business, the haunting feeling of death still lingered — virtually. Soon Roberston's internet was cluttered with gravestones. They followed her everywhere; she could not escape (Nudson, 2020). Robertson's story is not unique. In the wild west of the internet, companies are able to harvest user data and use it to serve personalized advertisements in the form of targeted advertising. This practice is harmful to individuals, yet companies (and even governments) use these technologies because they are profitable and effective.

The Issues

Data is being collected in droves, and despite some users' attempts on limiting the sharing of this information, it is almost impossible to use online services without sharing some data (Callanan et al., 2021). For example, even if one were to disable many tracking settings and delete all cookies before switching websites, advertisers would still be able to track the user across multiple sites through information such as the user's screen resolution, what web browser they are using, what version of web browser the user has, and what operating system is installed. This information can be compiled into a profile for that given user which is used to track their activity across multiple sites (Callanan et al., 2021).

However, most people do not even bother to go through with such rigorous privacy settings. This allows advertisers to open the flood gates on a targets' information. One advertiser, Meta Platforms Inc. (formally known as Facebook) reportedly, "provides ways to target geographic locations, personal interests, characteristics and behavior, including activity on other internet services and even in physical stores" (Callanan et al., 2021, p. 157). Advertisers can use this information to build a very detailed profile of a user including "their political affiliation; how likely they are to engage with political content; whether they like to jog, hike or hunt; what kind of beer they like; and so on" (Callanan et al., 2021, p. 157).

Advertisers do not collect all this information without reason. There are many strategies advertisers use to make their ads successful on a target. Thanks to the work of many academic researchers, advertisers know exactly what mood, content, and context any given ad must contain to be successful on a given site (Voorveld et al., 2018). For example, Twitter users engage with an ad if they view it as being informative, while users on YouTube view ads more negatively when using the platform for entertainment. These incredibly detailed measurements were made from the outside looking in, as the researchers were limited to asking a relatively small number of users simple questions to get their data (Voorveld et al., 2018). The tools companies have for analyzing their internally generated data are many times more accurate, thus allowing companies to effectively maximize the use of massive amounts of data their users produce.

There is also evidence that some governments are taking advantage of targeted advertising in order to change their respective population's behavior. Such activities raise serious moral and ethical concerns. One study found that the UK government was actively using the same targeting systems companies use to encourage and discourage certain types of behavior (Collier et al., 2022). This activity ranged from targeting adolescents who looked up illegal topics with messages and warnings of punishment to showing fire safety ads to people who recently bought candles. There are even cases of the government using local community leaders in advertisements in order to better connect with targets. Understandably, this activity raises many moral and ethical questions, such as "Is it democratic for governments to be influencing behavior in this top-down approach?" and "Is it ok for the government to counter disinformation or should that be the responsibility of the population?" (Collier et al., 2022).

Targeted advertising is harmful because it is exploitative. Advertising agencies have unfettered access to vast amounts of data, which they use advanced artificial intelligence (AI) to filter through and find emerging behavior patterns. These AIs are able to predict outcomes of consumer choices, predict future behavior, and even predict details about a person even if the person is not aware of it yet (Callanan et al., 2021). In a now infamous example, Target – a mainly brick and mortar retailer – collected and sourced loads of data and then compiled it into a "pregnancy prediction" score. Target used this score to predict the likelihood of a customer becoming pregnant and allowed Target to send the expecting mother coupons. Predictions were often very accurate even before the customer had set up a baby-shower registry with the company (Callanan et al., 2021). Target was even able to estimate the stage of a customer's pregnancy and thus supply them with relative coupons. These Orwellian-esque tactics are very concerning, and Target knew that. A Target executive spoke on the matter saying,

> [W]e found out that as long as a pregnant woman thinks she hasn't been spied on, she'll use the coupons. She just assumes that everyone else on her block got the same mailer for diapers and cribs. As long as we don't spook her, it works. (Callanan et al., 2021, p. 160)

Other agencies like Google, were able to predict a user's mood, emotions, and sell this information off to advertisers. Meta is no better, also allowing the sale of their user's information, such as whether or not teenagers were feeling "'insecure', 'worthless', or otherwise in need of a 'confidence boost'" (Callanan et al., 2021, p. 158). It is painfully obvious that this information can be easily used to manipulate and influence vulnerable people into making decisions, and most importantly – purchases that they most likely would not have made given a better state of mind.

If advertisers and governments know this behavior is harmful, then why do these agencies keep using these tactics? This question can be answered in two parts. First, many companies have legal requirements to make their stakeholders happy. Often, this means making the stakeholders richer by any means possible (Callanan et al., 2021). Second, laws surrounding this behavior are either very vague or non-existent. Therefore, if it is not illegal to use targeted ads, and it is also very profitable; so why not use targeted advertisements (Callanan et al., 2021)? One recent notable change is the passage of the General Data Protection Regulation (GDPR) in the European Union. The GDPR includes a right to be forgotten, and a right to access, and a right to be informed when it comes to personal data (GDPR, 2018). Hopefully, these recent changes can force companies and governments to change their manipulative behavior.

Ethics

There are many ethical implications that targeted advertising produces. One of the biggest ethical issues is where we draw the line on how much personal information parties can collect. The answers society provides will shape the future of privacy focused legislation. The GDPR proposes many reasonable first steps that will inevitably radically change the way companies handle data. For instance, the GDPR creates a "right to be forgotten" (GDPR, 2018). How does a company handle this responsibility? Does a user have to request that they be forgotten or is the right exercised automatically? What about the death of a user?

Governments also provide a whole new set of ethical questions when it comes to using targeted advertising. Collier et al. (2022) argue that using these technologies for influencing behavior should not be a top-down approach. Instead these tools should be given to the wider population in order to encourage change from the bottom up. However, there are some big risks to this stance. Radical groups could also use this hypothetical technology to spread hateful rhetoric. Thus, society would need an arbiter of what is allowed to be spread. These points require more research if we are to implement a similar system.

There is also an argument that the government should be able to use targeted advertising, as it has been very successful in the UK government. Over a six month period, a NCA campaign seems to have completely stopped all growth in the purchase of Distributed Denial of Service (DDOS) attacks (Collier et al., 2022). This is notable because during the same time period, sales of DDOS attack services rose internationally. However, since these government programs are targeted to prevent criminal behavior before it happens, it is hard to objectively show a link between the use of targeted advertising by the government and a decline in any given crime. As Collier et al. (2022) put it, "We are also aware that the effects of these campaigns may be exaggerated, misreported or have not been continued" (p. 6).

Solutions

One would assume that a majority of people are in support of regulation of this practice, and that would be a correct assumption. In fact, 91% of Americans think that companies are tracking some or all of online activity, and 77% also believe the same about the government (Auxier & Rainie, 2019). Public support is there, yet in the United States, the political scene may be less suitable for change. In recent years, political tensions have been sharply rising, thus making it a miracle even for bipartisan legislation to become law. However, the topic of regulating companies is far from by-partisan. A survey conducted by Pew Research (2019) found that 71% of Republicans (America's dominant conservative party) think Government is too involved in matters that should be left to the private sector, while 78% of Democrats (America's dominant liberal/progressive party) think the government should be doing more to solve problems. Even if there was a popular push for government regulation of targeted advertising agencies, it would inevitably be split on party lines and be very controversial.

Although it will be very challenging to pass legislation, it is the only way to make significant change a reality. This is because tech companies hold a lot of power in the United States' legal system. For example, in 2022 the lobbying group TechNet (which is partially made up of members of the "Big Four"), successfully neutered a right-to-repair bill in New York (Cunningham, 2022). However, there may still be hope. With the recent public suspicion of the very popular short form video site TikTok, it may be possible for privacy activists to carry this momentum into changing US policy. For example, during the hearings, the wider population learned details on how TikTok collected data. These strategies are not isolated to TikTok; many of the "Big Four" (Apple, Google, Microsoft, and Meta) also use these exact same strategies. It is worth noting that change is most likely going to be most influential in the United States, as that is where Apple, Google, Meta, and Microsoft (a.k.a the "Big Four") are located (Callanan et al., 2021). Since the "Big Four" control most of the targeted advertising market, any change in their host country will propagate throughout the rest of the internet and – to an extent – the rest of the Western world. Once the public is aware of this, it could potentially push lawmakers into drafting and passing more privacy focused laws.

Limitations

One major limitation of this research is the legality of the proposed legislation. This study did not look into any case law and combines research from multiple countries, each with similar, yet distinct, legal systems. A law that might work in the European Union would be unlikely to work in the United States. The European Union, however, continues to pioneer this legislation in their system, and hopefully the Americans take note. Another limitation is the fact that most of the literature around this topic only sources from Western, Educated, Industrialized, Rich, and Democratic (WEIRD) countries. As our current internet mostly ignores borders, it is worth considering how any changes will affect those who are not of one's country.

Conclusion

In conclusion, companies and governments are collecting user data and using it to craft personalized advertisements that manipulate targets. This practice is perpetuated by outdated laws and a drive for ever-increasing profit. These behaviors raise many ethical questions that will direct the future of targeted advertising. Solutions to discussed issues will need to be implemented via law for any change to occur. The author hopes that this paper will provide a jumping off point for future research.

References

Auxier, B., & Rainie, L. (2019). *Key takeaways on Americans' views about privacy, surveillance and data-sharing*. Pew Research Center. https://www.pewresearch.org/short-reads/2019/11/15/key takeaways-on-americans-views-about-privacy-surveillance-and-data-sharing/

Callanan, G. A., Perri, D. F., & Tomkowicz, S. M. (2021). Targeting vulnerable populations: The ethical implications of data mining, automated prediction, and focused marketing. *Business and Society Review, 126*(2), 155-167. https://doi.org/10.1111/basr.12233

Collier, B., Flynn, G., Stewart, J., & Thomas, D. (2022). Influence government: Exploring practices, ethics, and power in the use of targeted advertising by the UK state. *Big Data & Society, 9*(1), 205395172210787. https://doi.org/10.1177/20539517221078756

Cunningham, A. (2022). *New York governor signs modified right-to-repair bill at the last minute.* Ars Technica. https://arstechnica.com/gadgets/2022/12/weakened-right-to-repair-bill-is-signed-into law by-new-yorks-governor/

General Data Protection Regulation (GDPR) – Legal Text. (2018). General Data Protection Regulation (GDPR). https://gdpr-info.eu/

Nudson, R. (2020, April 9). When targeted ads feel a little too targeted. *Vox*. https://www.vox.com/the goods/2020/4/9/21204425/targeted-ads-fertility-eating-disorder-coronavirus

Pew Research Center. (2019). *2. Views of government and the nation.* Pew Research Center. https://www.pewresearch.org/politics/2019/12/17/views-of-government-and-the-nation/

Voorveld, H. A. M., van Noort, G., Muntinga, D. G., & Bronner, F. (2018). Engagement with social media and social media advertising: The differentiating role of platform type. *Journal of Advertising, 47*(1), 38-54. https://doi.org/10.1080/00913367.2017.1405754