

# Personalization and Privacy: Conflicting Views of Targeted Digital Advertising

A Sociotechnical Research Paper  
presented to the faculty of the  
School of Engineering and Applied Science  
University of Virginia

by

Kelcie Satterthwaite

April 6, 2021

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments.

*Kelcie Satterthwaite*

*Sociotechnical advisor:* Peter Norton, Department of Engineering and Society

## **Personalization vs. Privacy: Conflicting Views of Targeted Digital Advertising**

Targeted digital advertising utilizes consumer internet activity data to identify specific traits, interests, and preferences of a customer. Advertisers apply this information to present users with ads that align with users' apparent interests. As of 2017, targeted digital advertising made up the largest share of the advertising market, surpassing television and print ads (Plane et al., 2017). The advertising industry's transition to targeted strategies sparked a spirited debate over the social, economic, and ethical implications of this method (Marotta et al., 2017). Advocates of targeted advertising include corporations that specialize in web applications, such as Facebook and Google. These proponents cite increased advertising efficiency as the reason for their advocacy (Chen & Stallaert, 2010). Digital privacy advocacy groups criticize this method. These groups argue that the collection of detailed behavioral data can constitute an invasion of consumer privacy (EFF, 2019).

Consumer data's pivotal role in targeted digital advertising makes this method controversial. Web application companies, such as Facebook and Google, offer a free service in exchange for their users' data. This data, such as age, gender, interests, and cross-device online behavior is collected and categorized to create a profile for each user (Houser & Gregory Voss, 2018). If the user has not opted out of the service's data collection practices, Facebook and Google have access to users' location, search history, and the apps they frequently use. These companies can also draw conclusions about other consumer characteristics such as a user's political and religious affiliations, relationship status at a given point in time, and sleep schedule (Curran, 2018). Brands do not gain direct access to this data, rather they pay technology companies to display their ads to users that match their target audience (Houser & Gregory Voss, 2018). Digital privacy advocacy groups are concerned that this advertising method "enables

unparalleled invasions of privacy” (EFF, 2020). The general public also shares this sentiment. According to a Pew Research study, at least 65% of adults are “not confident” that records of their activity maintained by social media sites and search engine providers will remain private and secure (Madden & Rainie, 2015). In an environment where their beliefs and perspectives conflict with those of other stakeholders, how do proponents of targeted digital advertising promote their agendas? To persuade consumers and regulatory bodies to accept the data practices that fuel targeted advertising, web application companies appeal to users’ values in company statements, utilize strategic linguistic and design choices in their interfaces, and influence the development of data regulations.

## **Review of Research**

Researchers have investigated the methods opponents of targeted digital advertising use to advance their agendas. According to Maréchal (2020), opponents of this advertising method promote their interests by encouraging shareholders to hold large digital companies (i.e. Google) accountable for addressing the ethical impacts of their data collecting practices. Maréchal (2020) also concludes that establishing a federal privacy law is an effective method to regulate corporate use of consumer information. Todt (2019) suggests that requiring companies to develop transparent data privacy policies can lead to the responsible use of targeted digital advertising.

### **Agenda Advancement:** *User Value Appeal*

Companies that specialize in web applications, such as Google and Facebook, value data collection because of its ability to “provide better services to [their] customers” (Google, 2020). These companies utilize consumer data to maintain and improve their services, provide

personalized experiences, and measure their system's performance (Google, 2020). While they aim to improve their users' experiences, profit is the true motivation for technology companies' support of targeted advertising and data collection. Providing personalized services such as content and ads proves to be the most productive utilization of consumer data and the primary revenue stream for many web application companies. In 2020, advertising made up 97.9% of Facebook's total revenue and 81% of Google's total revenue (Tankovska, 2021; Johnson, 2021). By tailoring ads and content to each individual user, these companies are able to "show ads to people who are most likely to find [them] relevant" (Facebook, n.d.). This strategy improves user retention and ad click through rates, two metrics that influence a company's advertising revenue.

Web application companies have been criticized by users and lawmakers for their use of consumer data. Most notably, Facebook received scrutiny when its failure to keep users' personal information secure allowed Cambridge Analytica, a political consulting firm, to obtain the data of 87 million people without their consent (Zialcita, 2019). Cambridge Analytica used this data to influence several elections worldwide, raising concerns among lawmakers and users over technology companies' data collection practices. Corporations hoping to enjoy the benefits of consumer data utilization must convince their users and regulatory bodies that their data practices are acceptable.

To convince consumers of the benefits of corporate data collection, web application companies appeal to values and social trends that users care about, such as app personalization, improved user experience, and the small business movement. These companies often frame justifications for data collection practices in a light that highlights user benefit. According to Facebook (2020), they collect user information because they are "passionate about creating engaging and customized experiences for people." Google states that its use of data in the

advertising process allows users to engage with “ads that are uniquely relevant to them” (Chavez, 2018). Public statements from Big Tech firms often insinuate that the user experience would decline without targeted advertising. In a statement about the future of privacy in advertising, Facebook’s Erin Egan recalls the state of early stage online marketing: “online ads in the 1990s were spammy. I certainly remember having content blocked or overlaid with flashing, annoying ads” (Egan & Satterfield, 2020). She later states that over the years these “spammy experiences have subsided” (Egan & Satterfield, 2020) due to the rise of personalization (Egan & Satterfield, 2020). As personalized ads are uniquely relevant and interesting to the user, advertisers do not need to show flashing banners to get people’s attention. According to Egan, personalization makes it easier to show ads without disrupting the user experience, thus it provides the “best experience for people” (Egan & Satterfield, 2020). Egan’s comments aim to reassure users that targeted advertising and the data collection practices that power it, are the key to a positive online user experience. By highlighting user benefit and using imagery to convey their message, corporations are able to appeal to users’ values and subsequently shape public sentiment.

To garner consumer support for their cause, web application companies highlight their support of popular social movements. Public support for the small business movement reemerged during the 2020 COVID-19 pandemic. This movement encourages consumers to switch their spending from big-box stores to small businesses. The economic impacts of the pandemic forced many small businesses to close their doors. Between February and April 2020, the active number of business owners declined by 22%, marking the largest drop in business owners on record (Fairlie, 2020). Noticing that their local businesses were struggling, consumers encouraged their peers to “shop local”. According to the National Retail Federation, 49% of

consumers made a purchase or donation to support a local business during the pandemic (NRF, 2020). 41% of consumers intend to make this a long-term habit and will continue to buy locally in a post-pandemic world (Erdly, 2020).

Facebook, a company ranked number 46 on the 2020 Fortune 500 list (Fortune, 2021), has realized the power of local and its value to consumers. In response to Apple's enforcement of privacy regulations that hinder targeted advertising, Facebook released an article titled "Speaking up for Small Businesses". This press release states that Apple's new policies will "have a harmful impact on many small businesses that are struggling to stay afloat [during the pandemic]" (Levy, 2020). According to Facebook, the company's personalized advertising services allow businesses to "run a campaign with a phone and a few dollars" (Levy, 2020). By limiting online personalized advertising, Apple's policy will make it harder for small businesses, which have small budgets, to reach their target audience. Thus, limiting their growth and ability to compete with big companies (Levy, 2020).

To continue to show their support for small businesses, Facebook launched Good Ideas Deserve To Be Found. This initiative showcases people discovering businesses they love through Facebook and Instagram -- an event that is made possible with the use of personalized ads. The company also introduced policy changes that waive fees and extend payment windows for small businesses (Facebook, 2021). Similarly, Google has shown its support by committing \$340 million in Google Ads credits for small businesses worldwide. This commitment is a gesture meant to "show support and solidarity" with the small and medium sized businesses that are "the backbone of our communities" (Google, n.d.). Highlighting their support for popular social movements, such as the "shop small business" trend, allows web application companies to align themselves with consumer values in their public fight to protect targeted advertising.

## **Agenda Advancement:** *Strategic Linguistic Choices*

Web application companies' privacy policies include strategic linguistic choices that shape the extent to which user's understand the corporation's data practices. Readability studies illustrate that consumer-facing documents should be written at no more than an eighth-grade reading level. In contrast, a recent study indicates that of the 500 popular US websites tested, 498 of them had privacy policies and terms of service documents that required more than 14 years of education to understand (Benoliel & Becher, 2019). According to a 2017 Deloitte study, consumers are more likely to share their information if companies are "transparent about how they intend to use consumer data" (Deloitte, 2017). If transparency is the key to easing consumers' concerns, why are privacy policies written in legalese that is incomprehensible to the average user? Kit Walsh, a staff attorney with the digital privacy advocacy group the Electronic Frontier Foundation, argues that companies benefit from the unreadability of their privacy policies. She states that "the typical privacy policy doesn't say we will respect your privacy and not share your information. They're written to give the company as much leeway as possible" (O'Connor, 2018). The complex language present in privacy policies dissuades consumers from reading these agreements, shading them from the realities of corporate usage of their data (Benoliel & Becher, 2019).

Before 2018, web application companies succeeded in discouraging users from reading their full privacy policies and terms of service. A Deloitte study found that 91% of consumers accept legal terms and conditions without reading them (Deloitte, 2017). However, the publication of the Cambridge Analytica scandal in 2018 heightened user concerns about corporate data usage. To regain consumers' trust, web application companies increased the transparency of their privacy policies by adjusting the language used in these agreements. In its

updated agreements, Facebook removed legal jargon to provide users with an easy to read alternative to their traditional privacy policy documents (Facebook, n.d.). By being brief and readily understandable, this version of the privacy policy facilitated a transparent dialogue with consumers over data concerns (Rao & Dwivedi, 2017).

**Agenda Advancement:** *Strategic Design Choices*

Web application companies pair their promotion of user responsibility with dark interface patterns to give consumers a false sense of control over their data. In a digital privacy context, user responsibility signifies that users have the authority to control the information they share, but they must be proactive in doing so. In a statement about personalized advertising, Facebook states that they are committed to “respecting privacy and empowering people to control their information online” (Egan & Satterfield, 2020). Similarly, Google’s privacy policy states that users have “control over the information [Google] collects and how it’s used” (Google, n.d.). While these messages may reassure users, an analysis by the Norwegian Consumer Councils indicates that companies have little intention of actually giving users choices (Kaldestad, 2018).

Facebook and Google use dark patterns to suppress users’ control of their data and push them to select privacy intrusive options. Dark patterns are features of an interface designed to nudge users to take actions that are against their interests. Examples include strategically selected default settings, intentionally complex layouts, and incentives. Research shows that users rarely review or change an interface’s default settings, making the preselection of these settings an effective method to nudge users. Correspondingly, Facebook and Google’s standard settings are pre-set to the least privacy friendly options (Kaldestad, 2018).



Intentionally complex interface layouts make activating privacy friendly choices difficult (Kaldestad, 2018). The “accept and continue” button on Facebook’s interface allows users to select the default settings (the most privacy intrusive options) with one click. In contrast, activating privacy friendly options requires 13 clicks. Users open Facebook accounts because they want to use the service, not because they want to spend copious amounts of time selecting privacy settings. By making the easiest path to using the service one that includes accepting the default settings, web application companies nudge users to share most of their data (Kaldestad & Myrstad, 2018).

Web application companies incentivize user decisions that align with the company’s agenda and punish those that do not. Incentives include extra functionality and a better user experience, while punishments are presented as “take it or leave it” situations. More specifically, Facebook and Google’s interfaces threaten users with the loss of functionality or deletion of their account if they opt out of the privacy intrusive option. A screen detailing Facebook's new privacy terms presented users with two options: accept the updated policy or “see your options”. The “see your options” button led users to an ultimatum: go back and accept the terms or delete your account (Kaldestad & Myrstad, 2018). Similarly, users that opted to turn off Google's ad personalization features were presented with a screen that warned them that they “will still see ads, but they will be less relevant to [them]” (Kaldestad & Myrstad, 2018). Threats of an unpleasant experience or the loss of the opportunity to use the service pushes users to share their information.

### **Agenda Advancement:** *Legal Initiatives*

To ensure their interests are legally protected, web application companies seek to influence data privacy regulations. The United States does not have a comprehensive federal law that governs data privacy; rather it is handled on a sectoral basis. This sectoral approach does not provide distinct regulation of tech companies' data practices (Houser & Gregory Voss, 2018). Despite the lack of federal regulation, there are numerous state laws that intend to protect consumers' privacy online. California's Consumer Privacy Act (CCPA), effective January 2020, is the most robust state data privacy law to date (Harwel, 2019). This legislation gives consumers significant control over the personal data businesses collect (Office of the Attorney General, n.d.). California's Consumer Privacy Act mimics the European Union's (EU) General Data Protection Regulation (GDPR), a legislation that coordinates data privacy laws across all EU countries and gives consumers more control over their information. The GDPR "strengthens citizens' right to say how data about them can be used, giving them the power to correct, delete and freely move their information from one service to another" (Scola et al., 2018).

To shape the consumer privacy standards that will be determined by future legislations, technology companies show their support for comprehensive privacy regulation. According to Facebook's Erin Egan, the company hopes to "work collaboratively with policymakers, regulators, and others in the industry on policy regimes that ensure strong privacy protections" (Egan & Satterfield, 2020). In an early 2020 article titled "Big Tech Needs More Regulation" Facebook's CEO, Mark Zuckerberg, argues that there is a need for additional regulation in the tech world as "private companies [shouldn't] make so many decisions alone when they touch on fundamental democratic values" (Zuckerberg, 2020). Welcoming new regulations with open arms gives tech companies the opportunity to shape these new policies and ensure they serve

their interests. In his “Big Tech Needs More Regulation” press release, Mark Zuckerberg also highlights specific themes new regulation should cover: transparency, openness, data portability, and oversight and accountability (Zuckerberg, 2020). It is not a coincidence that many of these themes are requirements Facebook already meets.

Tech companies' support for data privacy laws is conditional on lawmakers' willingness to include them in the development of new legislation. In a white paper about ways tech companies can communicate with users about their privacy rights, Facebook states that the best method to develop policies governing data practices is policy co-creation, a process in which regulations are created through the collaboration of policymakers, companies, and other experts (Egan, 2020).

Lobbying is another method web application companies use to influence the legal privacy debate. According to Daniel R. Stoller of Bloomberg Law, tech companies have donated to “support highly influential think tanks and public interest groups that are helping shape the privacy debate, ostensibly as independent observers” (Stoller & Dunbar, 2019). These interest groups include the Center for Democracy and Technology, the Brookings Institution, and the Future of Privacy Forum, all of which have influence over legislators, journalists, and the public. Despite their claims that donations do not influence their views or decisions, these organizations often push positions that favor their donors, Google and Facebook (Stoller & Dunbar, 2019). Accordingly, tech companies have substantially increased their spending on lobbying. Before 2010, Facebook’s highest one-year total spent on lobbying was \$200,000, while Google’s was \$1.5 million. By the end of 2018, Facebook and Google spent \$12.6 million and \$22 million on lobbying respectively (Stoller & Dunbar, 2019). By influencing the development of new data

privacy regulations, web application companies are able to prevent future legislations from hindering their targeted advertising practices.

### **Conclusion: The Relationship Between Corporations and Society**

Web application companies advance their agendas by shaping the beliefs and perspectives of other stakeholders. In this approach, these companies employ direct and indirect strategies to convince others that their data practices are acceptable. These methods are not limited to web application companies' efforts to protect targeted advertising and its monetary benefits. Rather, their approach shines light on corporations' ability to shape societal standards. As the targeted advertising use case displays, large companies have a significant influence on consumers and regulatory bodies. A company's development of a new technology, such as the smartphone, can spark shifts in consumer behavior. According to traditional business principles, companies should protect the interests of their shareholders at all costs. However, when a business' product or service has the potential to provoke societal change, these corporations must consider more than just the interests of their shareholders, they must also account for the general public. As seen in Facebook and Google's targeted advertising crusade, corporations can often successfully shape the decisions of consumers and regulatory bodies. Thus, before employing their persuasion techniques, these influential companies must consider the impacts their agendas may have on society. They must ask themselves if the advancement of their agendas aligns with the greater societal good.

## References

- Benoiel, U., & Becher, S. I. (2019). The Duty to Read the Unreadable. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.3313837>
- Chavez, A. (2018, August 27). Create more effective ads for today's consumer [Web log post]. <https://blog.google/products/ads/create-effective-ads/>
- Chen, Jianqing and Stallaert, Jan, An Economic Analysis of Online Advertising Using Behavioral Targeting (August 1, 2010). *MIS Quarterly*, 38(2), 429-449, 2014., Available at SSRN
- Curran, D. (2018, March 30). *Are you ready? This is all the data Facebook and Google have on you*. The Guardian. <https://www.theguardian.com/commentisfree/2018/mar/28/all-the-data-facebook-google-has-on-you-privacy>.
- Dark Patterns. (n.d.). <https://www.darkpatterns.org/>.
- Deloitte. (2017). *2017 Global Mobile Consumer Survey: US edition*. Deloitte. <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology-media-telecommunications/us-tmt-2017-global-mobile-consumer-survey-executive-summary.pdf>.
- EFF (2019, June 3). Electronic Frontier Foundation. About EFF. <https://www.eff.org/about>
- Egan, E., & Satterfield, S. (2020, October 2). A Path Forward for Privacy and Online Advertising [Web log post]. <https://about.fb.com/news/2020/10/a-path-forward-for-privacy-and-online-advertising/>
- Egan, E. (2020, July). *Communicating About Privacy: Towards People-Centered and Accountable Design*. Facebook. <https://about.fb.com/wp-content/uploads/2020/07/Privacy-Transparency-White-Paper.pdf>.
- Erdly, C. (2020, December 18). *Four Trends That Will Shape Retail In 2021*. Forbes. <https://www.forbes.com/sites/catherineerdly/2020/12/18/four-trends-that-will-shape-retail-in-2021/?sh=66c04eda5add%29>.
- Facebook. (2021, February 25). *Let's Talk About Why Personalized Ads Matter*. Facebook. <https://about.fb.com/news/2021/02/lets-talk-about-why-personalized-ads-matter/>.
- Facebook. (n.d.). Facebook advertising targeting options. <https://www.facebook.com/business/ads/ad-targeting>
- Facebook. (n.d.). *We're Making Our Terms and Data Policy Clearer, Without New Rights to Use Your Data on Facebook*. Facebook. <https://www.facebook.com/about/terms-updates>.

- Fairlie R. (2020). The impact of COVID-19 on small business owners: Evidence from the first 3 months after widespread social-distancing restrictions. *Journal of economics & management strategy*, 10.1111/jems.12400. Advance online publication. <https://doi.org/10.1111/jems.12400>
- Fortune. (2021, January 25). *2020 Fortune 500: Facebook*. Fortune. <https://fortune.com/company/facebook/fortune500/>.
- Google. (2020, September 30). Privacy Policy – Privacy & Terms. <https://policies.google.com/privacy>
- Google. (n.d.). *COVID-19: Ad credits for Google Ads Small and Medium-sized Businesses*. Google Ads Help. <https://support.google.com/google-ads/answer/9803410?hl=en#zippy=%2Cwhy-is-google-offering-ad-credits-to-small-and-medium-businesses>.
- Google. (n.d.). *Privacy Policy – Privacy & Terms*. Google. <https://policies.google.com/privacy?hl=en-US#infochoices>.
- Harwel, E. F. (2019, October 7). *What Businesses Need to Know About the California Consumer Privacy Act*. American Bar Association. [https://www.americanbar.org/groups/business\\_law/publications/blt/2019/10/ca-consumer-privacy/](https://www.americanbar.org/groups/business_law/publications/blt/2019/10/ca-consumer-privacy/).
- Houser, K. A., & Gregory Voss, W. (2018, November 6). *GDPR: The end of Google and Facebook or a new paradigm in data privacy?* <https://jolt.richmond.edu/gdpr-the-end-of-google-and-facebook-or-a-new-paradigm-in-data-privacy/>.
- Johnson, J. (2021, February 05). Google: Ad REVENUE 2001-2018. <https://www.statista.com/statistics/266249/advertising-revenue-of-google/>
- Kaldestad, Ø. H. (2018, June 27). *New analysis shows how Facebook and Google push users into sharing personal data*. Forbrukerrådet. <https://www.forbrukerradet.no/side/facebook-and-google-manipulate-users-into-sharing-personal-data/>.
- Kaldestad, Ø. H., & Myrstad, F. (2018). (rep.). *Deceived by Design*. Forbrukerradet. Retrieved from <https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf>
- Levy, D. (2020, December 16). *Speaking Up for Small Businesses*. Facebook. <https://about.fb.com/news/2020/12/speaking-up-for-small-businesses/>.
- Madden, M., & Rainie, L. (2015, May 20). *Americans' Attitudes About Privacy, Security and Surveillance*. Pew Research Center: Internet, Science & Tech.

- <https://www.pewresearch.org/internet/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/>.
- Marotta, V., Zhang, K., & Acquisti, A. (2017). The Welfare Impact of Targeted Advertising. [https://www.heinz.cmu.edu/~acquisti/papers/Acquisti\\_Welfare\\_Impact\\_of\\_Targeted\\_Advertising.pdf](https://www.heinz.cmu.edu/~acquisti/papers/Acquisti_Welfare_Impact_of_Targeted_Advertising.pdf)
- National Retail Federation. (2020, April 22). *3 ways the coronavirus is impacting consumers' shopping behavior*. National Retail Federation. <https://nrf.com/blog/3-ways-coronavirus-impacting-consumers-shopping-behavior>.
- O'Connor, A. (2018, April 18). *Site Hopes to Cure Terms of Service Confusion*. AARP. <https://www.aarp.org/home-family/personal-technology/info-2018/terms-of-service-ratings.html>.
- Office of the Attorney General. (n.d.). *California Consumer Privacy Act (CCPA)*. State of California - Department of Justice . <https://oag.ca.gov/privacy/ccpa>.
- Plane, A., Redmiles, E., Mazurek, M., & Tschantz, M. (2017). Exploring User Perceptions of Discrimination in Online Targeted Advertising. In 26th USENIX Security Symposium (USENIX Security 17) (pp. 935–951). USENIX Association.
- Rao, V., & Dwivedi, K. (2017, September 5). *To share or not to share*. Deloitte Insights. <https://www2.deloitte.com/us/en/insights/industry/retail-distribution/sharing-personal-information-consumer-privacy-concerns.html>.
- Scola, N., Cerulus, L., & Gold, A. (2018, May 25). *Tech scrambles to shape U.S. privacy debate as EU rules loom*. Politico. <https://www.politico.com/story/2018/05/25/tech-privacy-debate-us-eu-rules-565741>.
- Stoller, D. R. (2019, November 18). *Facebook, Google Fund Groups Shaping Federal Privacy Debate* . Bloomberg Law. <https://news.bloomberglaw.com/tech-and-telecom-law/facebook-google-donate-heavily-to-privacy-advocacy-groups>.
- Tankovska, H. (2021, February 05). Facebook ad Revenue 2009-2018. <https://www.statista.com/statistics/271258/facebooks-advertising-revenue-worldwide/#:~:text=In%202020%2C%20about%2097.9%20percent,increase%20in%20comparison%20to%20the>.
- Zialcita, P. (2019, October 30). Facebook pays \$643,000 fine for role in Cambridge Analytica scandal. <https://www.npr.org/2019/10/30/774749376/facebook-pays-643-000-fine-for-role-in-cambridge-analytica-scandal>
- Zuckerberg, M. (2020, February 18). *Big Tech Needs More Regulation*. Facebook. <https://about.fb.com/news/2020/02/big-tech-needs-more-regulation/>.