Published on *The National Law Review* https://natlawreview.com

Can Target Marketing Withstand Emerging Privacy Regulations? Litigation (and Time) will Tell

Article By:

Zarish Baig

Kristin L. Bryan

The world of digital marketing has grown exponentially in the last two decades. In fact, it was estimated that in 2020, despite the global pandemic, approximately $332.84 billion will be spent on digital advertising worldwide.[1] Not surprisingly, sophisticated algorithms (such as real-time bidding and programmatic ad buying) have been built in recent years to master the science of digital marketing and customer segmentation-aka target marketing. While none of the current U.S. privacy laws explicitly prohibit target marketing based on electronically obtained consumer data, this space is getting over populated, and over regulated, and the landscape is changing. And so we ask the obvious question, can target marketing withstand the emerging privacy regulations? Our answer is *probably*, with certain notable caveats.

Target marketing is an old but powerful marketing strategy.[2] It used to involve breaking consumers into defined segments where each segment shared some similar characteristic, such as, gender, age, buying power, demographics, income, or a combination of a few shared characteristics; then designing marketing campaigns based on the shared characteristic(s). Approaches have changed with the passing of time. Nowadays, target marketing has been narrowed to the point of defining every individual consumer or household, and designing marketing campaigns for each individual consumer or household. Target marketing is often the key marketing tool used to attract new business, increase sales, or strengthen brand loyalty.[3] Despite its success, with the massive amount of consumer data now being used to target consumers, and the emerging data privacy laws and regulations, marketers have to tread carefully to avoid getting themselves in (legal) hot water.

How do marketers access consumer data? And why is it potentially problematic?

Lets first address consumer data. Marketers can acquire data by themselves, (aka, “first party data”). This includes data from behaviors, actions or interests demonstrated across website(s) or app(s), as well as data stored in a business’ customer relationship management system (“CRM”).[4] By contrast, “second party data” or “third party data” is data acquired from another source. It could be someone else’s first party data, or it could be data collected by outside sources that are not the original collectors of the data.[5]

The most common method for obtaining consumer data (first, second or third party) over the internet has been through cookies stored on our digital devices.[6] (For a recent litigation involving the use of cookies in the context of kids' privacy rights see this prior post). Cookies are used to track the activities of devices as users visit particular web pages, allowing advertisers to build profiles of a device's online activities; these profiles can then be used to create targeted advertising tailored to the user of that device.[7]

Marketers are also able to obtain data through social media platforms. Most of us using social media are aware of the personal information we submit before we create our accounts. This information may include some personally "identifiable" information, such as our name, address, date of birth etc., but there is other personal information which is not considered "identifiable", such as our gender, age, postal code, etc. Marketers can then partner with social media platforms to create marketing campaigns based on consumer segments created through each individual's personal information. Ever wonder why your husband is not seeing ads for women's shoes, or why you are receiving ads for products or services you have not shopped for but ***may*** be interested in? It is target marketing. (And of course, as CPW has covered, data can also be harvested from social medial platforms through scraping).

So what? Well, until recently (with a few notable exceptions such as the Fair Credit Reporting Act ("FCRA")) laws regulating companies selling or acquiring consumer data were sparse and preceded the advent of new technologies. *Compare Trans Union LLC v. FTC*, 536 U.S. 915, 917 (2002) (stating that "the FCRA permits prescreening—the disclosure of consumer reports for target marketing for credit and insurance. . . .") *with FTC I*, 81 F.3d 228 (D.C. Cir. 1996) (holding that selling consumer reports for target marketing violates the FCRA).

In many respects, corporations were thus able to use consumer data to create complex marketing campaigns. This practice recently came up in the context of the Capital One data breach. *See, e.g.*, *In re Capital One Consumer Data Sec. Breach Litig.*, 2020 U.S. Dist. LEXIS 175304, at *28 (E.D. Va. Sep. 18, 2020) (discussing plaintiffs' allegation that "Capital One created a massive concentration of [personally identifiable information, a 'data lake,' in which Capital One 'mines [customers'] data for purposes of product development, targeted solicitation for new products, and target marketing of new partners—all in an effort to boost its profits.").

The tide is starting to change. With the emergence of more recent data privacy laws, such as the California Privacy Rights Act of 2020" ("CPRA"), the California Consumer Privacy Act of 2018 ("CCPA") and General Data Protection Regulation ("GDPR"), "covered entities" can no longer use personal information *carte blanche* for advertising purposes. However, it bears noting that the statutory definition of personal information remains much narrower than what one might assume. CCPA for example defines personal information as: "…information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household…" *California Consumer Privacy Act of 2018* §1798.140.(o)(1).

Thus, information about one's gender and income, without more, would not be fall under this definition. Are consumers comfortable to have this information used without their consent? Do they even have a choice? It depends. Although common law tort principles, such as invasion of privacy, embarrassment or emotional distress, may allow some legal remedies, case law is sparse and for obvious reasons, has trended towards permitting corporate use of such data. *See, e.g.*, *Bradley v. T-Mobile US, Inc.*, 2020 U.S. Dist. LEXIS 44102 (N.D. Cal. Mar. 13, 2020) (rejecting claim that use of consumer data, including age, for target marketing concerning online job postings constituted age

discrimination and violated various federal and state laws).

At least insofar as California is concerned, there has been some interesting developments concerning target marketing of late. This is because under CCPA, some businesses engaged in target marketing interpreted "sales" as excluding the exchange of personal information, such as cookie data, for targeting and serving advertising to users across different platforms. This approach was on the purported basis that no "sales" (as defined in the statute) were involved because no exchange for "valuable consideration" had occurred. The CPRA, which was approved by California voters in November, utilizes the concept of "sharing" and seemingly eliminates this potential loophole (although that doesn't mean there won't be future litigation regarding this issue).

The concept of "data clean rooms" as also (re)surfaced to bypass the issues related to sharing customer data. Data clean room allow companies, or divisions of a single company, to bring data together for joint analysis under defined guidelines and restrictions that keep the data secure[8]. Whether a clean room contains PII or anonymized data, data privacy practices are critical. If the anonymized data can be deanonymized (tied back to actual people through creative analytics), it would make the data subject to most privacy laws (and definitely the GDPR).

What does the future look like for digital advertising? With the spike in US state regulations relating to consumers' online privacy, such as, CPRA, the Nevada Senate Bill 220 Online Privacy Law (2019), and the Maine Act to Protect the Privacy of Online Consumer Information (2019)[9], it remains fluid. There has also been changes in cybersecurity, data security and data breach notification laws (although we will table discussion of the specifics of that for another day). The bottom line is that marketers now not only have to pay extra attention to each state's regulation before obtaining and/or processing consumer information, they also have to pay extra attention to the consent obtained. The free reigns of using unlimited consumer data to create complex algorithms for the optimal marketing campaign is slowly coming to a halt.

To mitigate litigation risk, entities in the marketing industry will have to take a jurisdiction specific approach that accounts for recent developments. And as the scope of these new laws and regulations are tested via litigation, CPW will be there every step of the way. Stay tuned.

[1] https://www.emarketer.com/content/global-digital-ad-spending-update-q2-2020

[2] https://www.acrwebsite.org/volumes/8572/volumes/v29/NA-29

[3] https://www.thebalancesmb.com/target-marketing-2948355

[4] https://www.lotame.com/1st-party-2nd-party-3rd-party-data-what-does-it-all-mean/#:~:text=First%20party%20data%20is%20the,you%20have%20in%20your%20CRM

[5] Ibid.

[6] Swire, Peter and Kennedy-Mayo, DeBrae, "U.S. Private-Sector Privacy," Third Edition, Pg 130

[7] *Ibid*.

[8] https://www.snowflake.com/blog/distributed-data-clean-rooms-powered-by-snowflake/

[9] https://www.csoonline.com/article/3429608/11-new-state-privacy-and-security-laws-explained-is-your-business-ready.htm

© Copyright 2025 Squire Patton Boggs (US) LLP

National Law Review, Volume XI, Number 6

Source URL:https://natlawreview.com/article/can-target-marketing-withstand-emerging-privacy-regulations-litigation-and-time-will