

In an age of targeted advertising, do we need stronger regulations to protect privacy of netizens?

TNIE [newindianexpress.com/web-only/2023/mar/29/in-an-age-of-targeted-advertising-do-we-need-stronger-regulations-to-protect-privacy-of-netizens-2560707.html](https://www.newindianexpress.com/web-only/2023/mar/29/in-an-age-of-targeted-advertising-do-we-need-stronger-regulations-to-protect-privacy-of-netizens-2560707.html)



Image used for illustrative purposes only. (Express Illustrations)

By [Nikhil Naren](#)

The ways in which consumers view advertisements have changed over time. Marketers are now using extremely updated tools to pitch their products to people who would be most tempted to purchase them. Such targeted advertising relies on personal data of users that is provided either by social media platforms, third parties who collect data from the primary collectors, or through other actors. However, what becomes most important to understand is the interplay between the use of such targeted advertisement mechanisms and the privacy of users.

Targeted advertisements cannot exist without online tracking and profiling of users. This takes us to the question of whether it is fundamentally necessary, proportionate and fair to undertake targeted advertising of individuals. From the perspective of data protection, online tracking can describe the various processing activities, undertaken by different means, and for different purposes. It is also worth noting here that online tracking can operate using both active and passive techniques. Active techniques could mean users handing out their data by themselves, while passive techniques could include derivation, observation and inferences. Therefore, it should not be difficult for us to conclude that online tracking using passive techniques can raise a more significant risk of harm.

The adtech industry has also taken a number of initiatives to shift towards less intrusive tracking mechanisms and profiling practices. Such a move is also welcome from the perspective of data protection. Some of the initiatives include phasing out the use of

“third-party cookies” and replacing them with other alternatives. Tech giant Apple recently introduced an “App Tracking Transparency” feature which allows users to block an application from tracking their activities. Such a move not only boosts the confidence of users exercising their control over being tracked, but also in the market itself. Other mechanisms enable individuals to select their privacy preferences.

ALSO READ | People branding: Showing them the good, bad and ugly

For instance, the United Kingdom’s Regulation 6(1) of The Privacy and Electronic Communications Regulations, 2003, states that "a person shall not store or gain access to information stored, in the terminal equipment of a subscriber or user." This is sometimes also known as the 'cookie law'. The evolution of cookies and their use for targeted advertising is a cautionary tale of the risks of repurposing technology without also building in safeguards to protect against misuse and harm.

In January 2019, the French Data Protection Authority (CNIL) slapped Google with a 50 million euros fine for breaches of the General Data Protection Regulation (GDPR), in response to complaints made by privacy campaign groups in relation to the use of targeted advertising in the Android operating system. Specifically, the CNIL found that Google had not complied with the transparency and information requirements under the GDPR in its privacy policy and had not obtained valid consent for targeted advertising because users were given insufficient information for their consent to be valid, informed and specific.

Marketers are trying out new possibilities for reaching out and connecting to their audiences through targeted advertising. Isn't targeted advertising becoming more about building one-to-one personal connections? Can these personal connections be built in compliance with data protection legislations? Presently, all these companies are relying on data sets and algorithms to target a similar set of consumers, and in practice the one size fits all approach may not yield profits for them.

On one end of the spectrum, coming up with privacy regulations such as the GDPR in Europe or the California Consumer Privacy Act in the US will also force companies to make a gradual shift from mass or spam marketing, and focus more on targeted programs.

ALSO READ | Regulating misleading advertisements

In India, while we have gradually started focusing on online marketing by regulating misleading and endorsing misleading advertisements, very little has been done in the space of online targeted advertising on the global front. A specialised regulation may be needed that incorporates the core-value of consumer consent before feeding the consumer data into various artificial intelligence-powered algorithms for profiling or labelling.

Therefore, stronger advertising regulations could be a boon not only from the point of view of customer privacy, but also from the perspective of businesses. The implementation of newer technologies (alternatives to cookie-based advertising) will keep

garnering the attention of authorities, in cases where potentially intrusive personal data is involved. Hence, companies should keep adhering to the three core principles of the data protection law for the time being -- transparency, lawfulness and accountability. However, in the present age of a data-driven economy, which has fuelled surveillance capitalism, placing mechanisms to ensure consumers' consent should be the foremost step.

(Nikhil Naren is a Chevening Scholar, author, Assistant Professor at Jindal Global Law School and Of Counsel at Scriboard, New Delhi)

Now we are on Telegram too. Follow us for updates