Personal Data Protection Bill, 2019: Will it rid us of pesky and creepy ads?

As the Joint Parliamentary Committee considers the Personal Data Protection Bill, 2019, MediaNama will publish a series of articles from legal experts focussing on the key aspects of the Bill and how they will affect users and companies. This is the seventh article in the series. Read our extensive coverage of the Bill here.

By Divij Joshi

Ever get the strange feeling you're being watched online? When a 'real-life' conversation about food cravings results in an eerily similar restaurant ad on a totally unrelated website? Welcome to the 'uncanny valley' of targeted advertising.

Targeted advertising is the goldfield of the contemporary internet — the revenue backbone of social media, search engines, e-commerce and all of the ubiquitous 'free stuff' that fights for our online attention. The practices behind this business model have some troubling implications for online privacy. An instructive post by Sajjan Poovayya and Priyadarshi Banerjee outlined how the data collection of social media intermediaries may be affected by India's forthcoming personal data protection law. The advertising ecosystem is inseparable from the online economy and social media in particular, and deserves some further interrogation. In this post, I want to unpack the practical application of the PDP Bill's provisions to an increasingly popular advertising business model known as Real Time Bidding.

What is Real Time Bidding?

Online advertisements are increasingly placed using programmatic or automated systems, which apply sophisticated algorithmic rules to place advertisements targeted specifically towards the individuals browsing particular online publishers. In order to 'improve' the targeting of a particular users (to sell more relevant or purchasable ads from an ad company's perspective), companies require personal information about the individual visitor. This information is collected via a number of online tracking mechanisms using a number of tools — including cookies, device or browser fingerprinting or the use of tracking pixels, which track browsing activity across the web. These may be tools implemented by the publisher, or by third-parties who use the publisher's system to place cookies.

In simplified terms, Real Time Bidding or RTB is the system by which this information is collected, analysed and used for the purpose of serving ads. The information collected by publishers and by cookies is first sent to 'supply side platforms' (SSPs), who operate alongside 'ad exchanges' to connect publishers (or users, rather) with advertisers. The information is incorporated by SSPs into a 'bid request', which is broadcast to advertisers who compete to land 'impres-

sions' to specific individuals, through a near-instantaneous auction mechanism where every individual user and their information is 'sold' to these advertisers (or their agents). For an advertiser looking for an ideal 'target', the more information they have about a user, the greater the price they are willing to pay to an ad exchange for placing an ad, or an 'impression' on that user. The supply side of the advertising ecosystem therefore has an incentive to collect as much information about individuals and ultimately profile them for the purposes of selling to advertisers. These processes are largely governed by industry standards such as Google's Authorized Buyer's Framework or the IAB's OpenRTB system. (This diagram gives a simplified version of different actors within an RTB framework.)

At each level of operation of the advertising ecosystem — from the time someone loads a website to the time that they receive a targeted advertisement, multiple players are interacting and engaging in complex processes for shunting and processing personal information across the internet. Sensitive information (the most valuable to advertisers) is tracked and shared across multiple actors and databases, profiles are created about individuals using algorithmic logics, usually without the informed and continuing consent of the data principles. This is antithetical to accepted principles of data protection, including the right to informational self-determination as a constituent element of the fundamental right to privacy under the Constitution of India.

The burning question is — how does the recently introduced Personal Data Protection Bill map onto this complex ecosystem? Does it protect online consumers from rampant data extractivism and profiling?

The Personal Data Protection Bill — Reform or Relapse?

The PDP Bill attempts to place individual choice and autonomy at the heart of the data protection regime. The foremost is the requirement of informed consent before personal data can be collected or processed, under Sections 7 and 11. Further, the Bill requires personal data to be collected and used only for specific and clearly defined purposes, and only to the extent necessary for such purposes.

The PDP Bill also includes certain additional protections against 'profiling', which is defined as data processing that analyses or predicts user behavior and attributes. Data pertaining to children (Section 16), as well as sensitive personal data (Section 15), may be prohibited or require additional safeguards against profiling. However, these safeguards will not kick in until the Data Protection Authority under the Bill notifies and makes such protections applicable.

The definition of Personal Data under the PDP Bill includes all information by which a natural person (an individual) is directly or indirectly identifiable, including inferences made about such individuals. Any information which allows an individual to be specifically targeted, whether online or offline, will fall within this definition. Generally, the information collected by the RTB system includes

identity information such as an IP Address, or the 'fingerprint' from a device or browser — which are squarely relatable to individuals and fall under the category of personal data. In addition, information such as location data, timezone or other information can similarly be combined to identify an individual, and such combinations would also fall under the scope of the PDP Bill. These categories of data are often also used to make additional inferences about an individual, for example, correlating location data to financial data. In addition, certain RTB protocols also collect information relating to political affiliations, health status, sex or sexual orientation. This information falls under a special category of data known as 'sensitive personal data', and for which there exist additional protections under the Bill (although these additional protections will need to be notified by the Data Protection Authority).

Most of the information collected under contemporary RTB systems can therefore safely be assumed to fall under the PDP Bill's scope.

Who is responsible for maintaining the protection of personal data?

The PDP creates two categories of data processors — the data 'fiduciary', which is defined as the entity which controls the purpose for which the data was collected and processed; and the data processor, who may process data on behalf of the data fiduciary. **The primary responsibility of data protection vis-à-vis a data subject is on the data fiduciary.**

Determining the roles and responsibilities of each entity involved is perhaps the biggest challenge for operators as well as consumers in the ad-tech scenario. The large number of entities determining the means and the purpose of collecting and processing data means that there will be multiple entities with the responsibilities of a data fiduciary for the same data subject. In addition, there are hundreds of other entities to whom information is 'broadcasted' in the 'bid request' for the purpose of returning an automated bid. **While Section 31 of the PDP Bill requires that every data processor working on behalf of the data fiduciary must enter into a contract for the same, with the hundreds of entities involved, this becomes effectively impossible.** Further, certain publishers or entities like data brokers or social media companies may also qualify as 'significant data fiduciaries' under Section 26-30, have additional obligation in relation to their data collection and processing.

For an ordinary web user, there are severe challenges to their ability to control personal data. The current mechanisms for consent are entirely unmanageable and impossible to comprehend, let alone control. Although mechanisms like the 'consent manager' sought to be introduced under Section 23 may go some way into rectifying this problem, it is no easy task to reign in the complex data flows permitted by the RTB system. For example, companies are attempting to comply with the requirement of 'notice and consent' by providing 'clickwrap' consent notices which mean that users are expected to read through hundreds of privacy

policies before following through on a publisher's webpage. Additionally, the algorithmic logic and specific data used to profile and classify individuals (ranging from inferences about financial status, to gender and sexuality and caste) are unknown to users, even though it may affect the nature of advertisements they receive. However, the dependence of internet commerce on programmatic ads means that users are left with a Hobson's choice — to 'consent', or to be locked out of the web.

Conclusion

Barring some exceptions, the provisions of the PDP Bill appear to severely curtain the collection, processing and sharing of personal data within the online advertisement space and under RTB. However, experience from Europe indicates that the very business model of online advertising may be fundamentally incompatible with requirements of informed notice and consent under data protection laws. As a recent study by Karolina Iwańska and Harriet Kingaby indicates, this model of online advertising may be fundamentally broken beyond repair.

RTB (and other forms of programmatic advertisements) may be antithetical to data protection inasmuch as it is driven by the requirement that personal information be collected and broadcast across hundreds or thousands of entities with no technical or governance mechanism to keep such data sharing in check. Such practices and their potential non-compliance with the GDPR are already coming under the scrutiny of various executive and judicial authorities, including the UK's ICO and Norway's consumer protection agency, which have categorically determined that RTB violates European and national data protection law, and urged for courts and governments to enforce law by intervening in the RTB system.

Any reform of programmatic advertising and its harms to users, under the PDP Bill, may ultimately be question of the DPA's capacity and willingness to enforce the principles of purpose limitation, informed notice and consent, as well as its ability to make progressive regulations to protect against individual profiling. The broader question however, is whether an internet economy rooted in capturing and monetising every iota of our attention can ever be compatible with our established and emerging norms of online privacy, and how the ad-tech system can embody principles of data minimisation and privacy by design in their technical and commercial choices.

*

Divij Joshi *is a lawyer and a legal researcher, currently researching artificial intelligence and automated systems, as a Mozilla Tech Policy Fellow. He can be reached on Twitter at @divijualsuspect.*

Edited by Aditi Agrawal