PRIVACY VS. POSNER – IN LIGHT OF BIG DATA ANALYTICS AND THE *SRIKRISHNA COMMITTEE* REPORT, 2018

Buddhi Nishita Gauri

Third Year, Law student
Christ (Deemed to be) University
Bengaluru, India

Abstract: ***The rise of the internet in the past decade has implications that were unfathomable when it dawned upon us. Today's infinitely complex and labyrinthine data ecosystem is beyond the comprehension of most ordinary users. Despite a growing willingness to share information online, most people have no understanding of what happens to their data. Data analysis has commercial implications and loss of privacy. It is only appropriate that the individual should be the one holding the reins and taking the large decisions about the use of his personal data. The unequal power in the system allures users with consent and thereby paves way for a trade-off between privacy and commercial interests.***

The recent Srikrishna Report aims at syncing law with the change in technology and has carved a way forward for India becoming the next big data power across the globe.

The relevance of Posner's critique of Privacy is also examined by placing his argument against all digital footprints that leaves the human mind naked before the world.

IndexTerms - Big Data, commercial interest, individual interest, trade-off, privacy

I. INTRODUCTION

"Google knows you more than your mom"; a phrase than lingered long after it was first heard. The rise of the internet in the past decade has implications that were unfathomable when it dawned upon us. The sheer dependence and the vesting of the human mind in an electronic device is a scary fascination. The idea that 'my mind' is no longer is just no longer within my grey cells is bewildering.

In light of the 2017 Judgment by the Honorable Supreme Court, in ***K S Puttaswamy v. Union of India***[1] – the nine judge bench unanimously upheld Right to Privacy as a fundamental right and Justice Sanjay Kishan Kaul has highlighted the privacy intrusion by non-state actors and the requirement of state intervention through a comprehensive legislation that is need of the hour.

II. WHAT CONSTITUTES PRIVACY AND BIG DATA?

There has undoubtedly been enormous literature in this regard and several jurists have propounded various definitions and essentials of privacy. Right from *Samuel D. Warren; Louis D. Brandeis* (in 1890) to *Daniel Solove*, all of which has been analyzed in the Puttaswamy Judgement.

Privacy could be as simple as a door to a bathroom stall and as complicated as a judicial procedure regulating government surveillance of a suspected terrorist. Privacy is as narrow as an individual's ability to control the disclosure of an identification number assigned to that individual and as disparate as the rules governing the invisible tracking of an individual's online activities for behavioral advertising purposes. Privacy relates to an individual's preference for a particular song and to protect his/her physical location from a stalker. [2]

Privacy as a concept is heavily debated and there comprises of ideas which lie in a spectrum. More discussion leading to more disagreement about its scope, necessity, best practices and definition. It is however possible and necessary to talk about privacy in the absence of such consensus and what is it, that a state should endeavor to protect in this 21st century and digital age.

Justice D Y Chandrachud through his illuminative opinion connects Privacy to the concept of civil liberty. "Privacy, in its simplest sense, allows each human being to be left alone in a core which is inviolable. Yet the autonomy of the individual is conditioned by her relationships with the rest of society. Those relationships may and do often pose questions to autonomy and free choice. The overarching presence of state and non-state entities regulates aspects of social existence which bear upon the freedom of the individual. The preservation of constitutional liberty is, so to speak, work in progress. Challenges have to be addressed to existing problems. Equally, new challenges have to be dealt with in terms of a constitutional understanding of where liberty places an individual in the context of a social order. The emergence of new challenges is exemplified by this case, where the debate on privacy is being analysed in the context of a global information based society. In an age where information technology governs virtually every aspect of our lives, the task before the Court is to impart constitutional meaning to individual liberty in an interconnected world. While we revisit the question whether our constitution protects privacy as an elemental principle, the Court has to be sensitive to the needs of and the opportunities and dangers posed to liberty in a digital world.[3]

To be able to draw an analogy, Privacy is akin to a zorbing ball. A fundamental right to Privacy, ensures a sphere of unrestrained activity; activity within the socio-political boundaries that seeks no interference. However, this zorbing ball has perforations, which impose restrictions and ensures that the certain activities cannot remain unrestrained. In an age of Big Data Analytics however, human activity is within a transparent ball. Digital footprints are perpetually visible in their entirety. Visibility to a state and non- state actor. This research paper primarily concerns itself with non-state actors who hold in their possession enormous data that is difficult to bring under the umbrella of

[1] 2017 10 SCC 1
[2] Online Privacy, Robert Gellman and Pam Dixon. Page 2
[3] K S Puttaswamy vs Union of India ,2017 10 SCC 1 ,para 2

regulation. While state actors are also placed similarly, it is relatively easier to carve exceptions to privacy and attribute liability in case of breach of duty.

The absence of sound data protection laws and the lack of informational privacy has questioned the immense trust that people of the internet place in non-state actors .This paradigm is contrasted against the state who is expected to act in furtherance of the interests' of its citizens and yet is questioned (rightfully) about its activities in doing the same.

2.1 Big Data, Big Problems

Today's infinitely complex and labyrinthine data ecosystem is beyond the comprehension of most ordinary users.

But back in the early 1990s, online meant what is now the old-fashioned internet. The internet back in that time was essentially a not network of web pages but of interconnected computers that displayed screens of text. Today online has a much broader connotations. In the most technical sense, online refers to computers or devices that connect to the internet and the World Wide Web. There are many flavors and varieties of how a device can be online in this sense.

From desktop and laptops that can be online via modems, broadband, cable, etc. to sophisticated Cloud Computing would, the meaning of "online" has transformed in the past decade to being unrecognizable by its inventors.[4]

Habituated to frequent decisions that Artificial Intelligence makes on an individual's behalf, it isn't surprising that those decisions are not too different to the ones an individual would make for himself. [5] You Tube suggestions, Netflix match percentage, traffic alerts are miniscule examples of the manner in which Big Data plays a significant role in almost most decisions we take.

With the availability of big data, predictive analytics uses algorithms to recognize data patterns and predict future outcomes .Predictive analytics encompasses data mining, predictive modeling, machine learning, and forecasting.[6] The aim of such analysis is to identify relationships among variables that may not be immediately apparent using hypothesis-driven methods.

In 2011 it was estimated that the quantity of data produced globally would surpass 1.8 zettabyte and by 2013 that had grown to 4 zettabytes. With the nascent development of 'Internet of Things' gathering pace, these trends are likely grow exponentially. This expansion in the volume, velocity, and variety of data coupled with the development of innovative forms of statistical analytics, has big benefits and big concerns. [7]

Big Data processing is widely understood as comprising four stages: first, data collection from volunteered, observed, inferred or legally mandated data sets. This may or may not be limited to personal data sets; second, its storage and aggregation at scale; third, analyzing such aggregated data through machine learning; fourth, its use for prediction or targeting. Through these four stages, it is evident that data that is processed as well as the results from such data, may or may not relate to identified individuals.

There is enormous optimism pertaining to the benefits of Big Data when weighed against the concerns that weigh Big Data down. The concerns that weigh Big Data down is lesser in number but heavier in nature.

Improved decision making, better efficiency and productivity, convenient research, development and innovation accompanied by personalized search are some of the undisputable benefits of Big Data. All of which can be weighed against ***privacy*** where there can be lack of purpose limitation, notice and consent, opt-in-out and security. This shall be further discussed in the subsequent part of this paper.

While the Honorable Supreme Court has upheld the Right to Privacy it also emphasized the lack of state intervention in protecting informational privacy of its citizens and reiterated the importance of doing so. The said right would remain a dead letter in law, if non- state actors are not brought under the umbrella of regulation, when they could potentially be bigger flouters of privacy. The following section seeks to examine the weigh balance between commercial interests and individual interests, in a tradeoff.

III. COMMERCIAL INTERESTS V. INDIVIDUAL INTERESTS – IN A TRADEOFF

3.1 Changing Paradigm

The Government of India has recently released a report, after much deliberation by a high level panel constituted to examine and draft a Data Protection Bill. The committee was guided under the chairmanship of *Justice Srikrishna*, and the Bill is accompanied with the 276 report titled "A free and Fair Digital Economy, Empowering Indians". This report comprehensively illustrates the facets of informational privacy and also the stand that India shall take with regard to the same in comparison to the other nations with privacy laws already in force.

The report broadly describes three approaches to data Protection which is a reflection of the relationship that each state has with its citizens.

The US follows a *laissez-faire* approach and does not have an overarching data protection framework apart from the collectively recognized right by the US courts reflected through the First, Fourth, Fifth and Fourteenth framework to the US constitution. This is based on the approach that liberty is freedom from state control. Data protection is thus an obligation primarily on the state and certain categories of data handlers who process data that are considered worthy of public law protection.

The EU, on the other hand is at the vanguard of global data protection norms has recently enacted the EU GDPR, which has come into force on 25 May 2018. This is a comprehensive framework that covers all kinds of procession of personal data while illustrating the rights and obligations

[4] Online Privacy , Robert Gellman and Pam Dixon, page 3

[5] Leak of Faith, Navin J. Anthony – The Week April 8 2018

[6] Predictive Policing: What is it , How it works and its legal implications, Rohan George , available at <https://cis-india.org/internet-governance/blog/predictive-policing-what-is-it-how-it-works-and-it-legal-implications> last visited 14 Sept 2018

[7] Benefits and Harms of Big Data , Scott Mason , available at <https://cis-india.org/internet-governance/blog/benefits-and-harms-of-big-data> last visited on 14 September 2018

It is a comprehensive legal framework that deals with all kinds of processing of personal data and characterizes rights and obligations of parties in detail, to protect the privacy of Europeans in all its facets. This is founded on the need for the state to act as a facilitator in upholding the individual's dignity and therefore has stringent laws in place.

Despite these approaches that have dominated global thinking on this subject, China articulated its own approach which on the lines of averting National Security risks; with strict controls on cross-border sharing of personal data. The state frames its law keeping the collective interests over the individual interests and, the state privileges itself over the individual.

Each of these Paradigms above does not represent the citizen-state relationship that exists in India- which is based on two planks. First, that the state is a facilitator of human progress and it is directed by the DPSP to serve the common good. Secondly, that the state is prone to excess and is therefore checked by effectuating a vertical and horizontal separation of powers ,as well as Fundamental Rights that can be enforced against the state.

It is often perceived that economic growth and data protection are antithetic to each other, however this report aims to concur the two parallel lines that are presumed to never meet.

The inadequacy of regulation in the sphere of Data flow is a consequence of a simplistic assumption that data flows are an unadulterated good. The consequences of such assumption can cause significant harm, as exposed by the recent data sharing practices that Facebook demonstrated. This illustration represents the relationship between the Facebook and its users where Facebook holds the dominant position.

The Srikrishna Committee Report however, wishes to reverse this position, by making the individual the *"data Principal"* and the institute in whose confidence such data resides, the *"data Fiduciary"* .The objective being – to incorporate fairness and change the dimensions of inequality and grant bargaining power between persons who utilize such services.

The relationship between the individual and entities with whom the individual shares her personal data is one that is based on a fundamental expectation of trust. Notwithstanding any contractual relationship, an individual expects that her personal data will be used fairly, in a manner that fulfils her interest and is reasonably foreseeable. This is the hallmark of a fiduciary relationship[8]

3.2 Is Consent Opaque?

Understanding consent forms are a herculean task; for they are written for lawyers, by lawyers, with the tiniest of alphabets and incomprehensible clauses.

The problem with regard to consent is twofold in nature, firstly that consent forms are manufactured and designed to make the Non-State actor receive consent. Secondly, that users do not understand the implications of consent that are granted with utmost convenience.

Why is consent necessary*?*

The Srikrishna Committee illustrated two advantages – first, it respects user autonomy; second, it provides a clear basis for the entity to whom consent is given to disclaim liability regarding matters to which such consent pertains.[9]

There is however a vast difference between what consent ought to be and what it currently is.

The privacy paradox can be described as the phenomenon where an individual expresses strong privacy concerns but behaves in a contradictory way to these concerns. This flows from the economic concept that rational individuals are willing to give up information about themselves when they see benefits arising out of such a transaction.[10] If privacy were to be viewed as a commodity or a product, consent is a trade-off between privacy and efficiency.

Customized ads to predictive words suggestions on G-Board are best examples of the aforementioned contention.

If the above mentioned view is further taken into consideration, then the existing consent forms and *nudging* should be acceptable. If privacy is viewed as a product, then there can be two defects that the "consent" suffers from. Manufacturer's liability which is about the incomprehensibility of consent forms and Designer's liability where 'nudging of the user' is an example.

In order to tackle the manufacturer's liability, consent forms can be reduced to a "Data Trust Score". In addition, an alternate method can be user friendly videos which translate the consent forms While You Tube can make its viewer watch compulsory ads, a similar endeavor can be pursued to ensure complexity is broken down to simplicity. Google's privacy policy[11] has user-friendly videos which explains their privacy policy and its applicability. It is not mandatory, and similar practices must be undertaken by other Non-State Actors as well.

Nudges are considered to follow the soft or libertarian paternalism approach, where the user is not forbidden any options but only given a push to alter their behavior in a predictable way. [12] Acceptance or rejection of cookie policies on websites are mostly examples which make it intuitive for users to change settings and secure their data.

Nudging can be a privacy-enhancing tool or a privacy-compromise tool. Visual designs which "Accept" the terms and conditions are in bold blue and can positively influence the user to accept the terms and conditions, while "reject" is usually sober colors that the eye diverts lesser attention to.

Manufacturers do not exhibit accountability when the use of nudges is not directed at the wellbeing of its users. Visual notices must fulfill their primary purpose of meaningful communication. [13]

---

[8] Srikrishna Committee Report ,page 8

[9] Srikrishna Committee Report ,page 34

[10] State of the Information Privacy Literature: Where are We Now And Where Should WeGo?
Author(s): Paul A. Pavlou
Source: MIS Quarterly, Vol. 35, No. 4 (December 2011), pp. 977-988

[11] Available to everyone who has a Gmail account

[12] Privacy Nudges for Social Media: An Exploratory Facebook Study, available at <https://www.andrew.cmu.edu/user/pgl/psosm2013.pdf>

[13] Use of Visuals and Nudges in Privacy Notices, by Saumyaa Nayudu <https://cis-india.org/internet-governance/blog/use-of-visuals-and-nudges-in-privacy-notices> last visited on 15 Sept 2018

3.3 When the product is free, you are the product that is being sold

This is the aphorism that goes with the economic concept of "There is no such thing as a free lunch"
The following illustration is an example of how You Tube manages its ads and the revenue it generates.
Example: While watching a You-Tube video, a viewer watches an advertisement before the video commences (either under compulsion or otherwise). How did that particular video get to the viewer and how much money was involved in such target advertisement?
There are essentially three players in this scenario, creators who create videos, advertisers who make the Ad and You Tube who plays matchmaker between the other two players.
Unlike old dying media where an individual in a room could place Ads on a predictable known content at a leisurely schedule, You Tube doesn't and cannot work in a similar manner.
At any given point in time, a viral video may appear and on a normal day 65 years' worth of video are uploaded online. Endless waterfall of random content keeps growing. Hiring humans to categorize all those videos and match ads would be impossible. Therefore, this herculean task is undertaken by bots.
The moment each new video is uploaded ,You Tube bots get to work looking at the title, the keywords, the captions, the comments, the controversy – all to make their best guess as to what category it belongs.
Advertisers tell their own bots what kind of videos they want their ads to run against and what kind to avoid. Here is where You Tube earns their money – between when you click on a video and when it plays a You Tube bot holds an auction.
Announcing the categories it's guessed the video is in, opening the floor to all interested advertiser bots to place their bets.
The winning advertiser bot is the one with the ad that will most likely make You Tube and the creator the most money at that instant. But that is not necessarily the highest bidder- different ads pay different ways. For example, skippable video ads, the advertiser doesn't pay if the viewer skips as soon as they can. The advertiser pays only if their ads is clicked or watched.
A super high bid is worth less if the content is uninteresting. , no clicks translates to no revenue to the creator and You Tube. Auctioneer bot will prefer lower bid rate with higher click rate as against a higher bid rate for a lower click rate.
Uninteresting lies in the eyes of the beholder. Therefore in addition, to You Tube's bot guessing what the video is about, there are bots trying to guess what the viewer about. Looking at their watched history, device, activity, bots try to figure out and guess the viewer's age, locations, interests, chromosomes etc. This information is too a part of the auction and advertisers can instruct their bots to only bid to specific demographics in specific locations in specific categories and specific amount.
The entire transaction happens in around a millisecond. The subsequent revenue is split between You Tube and the creator.
Google collects information to provide better services to all its users- from figuring out basic stuff like which language the user speaks, to more complex things like which ads are the most useful, to the people who matter most to you online.
They collect information about activity undertaken while using their services, The activity information they collect may include:

- Terms searched for
- Videos watched
- Views and interactions with content and ads
- Voice and audio information when audio features are used
- Purchase activity
- People with whom users communicate or share content
- Activity on third-party sites and apps that use their services
- Chrome browsing history users have synced with their own Google Account

Google uses various technologies to collect and store information, including cookies, pixel tags, local storage, such as browser web storage or application data caches, databases, and server logs.
This illustrates that the digital footprints are left behind like trail that directs the "data fiduciary" to do what its users want best, at the cost of privacy.

IV. PRIVACY V. POSNER

Having understood privacy through the lens of its supporters, it is important to also not eliminate Richard Posner who critiques privacy at its best.
Richard Posner, in **'the Economics of Justice'** published in 1981, argued that privacy is protected in ways that are economically inefficient.[14]
Posner makes two distinct claims about privacy while defending the NSA and the profiling activities that it undertakes. *First*, he contends that machines cannot by themselves invade privacy; only other humans can .This claim is based on the argument that had the National Security Agency employed human beings to undertake the exact same activity that currently is undertaken by machines, then Posner implicitly concedes that there is an invasion of privacy. Collection and processing of private communications by an intelligence officer would involve the element of ***human sentient*** and therefore will be a breach of privacy.
Hence the importance of Posner's *second* claim, which is that the NSA's vacuuming up of personal data through electronic means can safeguard privacy by reducing the amount of human review. [15]
If this argument is extended to Big Data Analytics, which is similar to the nature of the task undertaken by the NSA, there essentially cannot be a breach of privacy. It is undoubted that this argument cannot sustain in its entirety, but it also cannot be disregarded.

V. CONCLUSION

Understanding the nature of privacy in the context of a digital world, is all the more necessary in the twenty first century. Having begun this article with the comparison of privacy to a zorbing ball, it must be reiterated that the comparison is profound for, the nature of digital

[14] K S Puttaswamy vs Union of India ,2017 10 SCC 1 ,para 140
[15] Privacy-Privacy Tradeoffs, David E. Pozen, The University of Chicago Law Review, Vol. 83, No. 1 (Winter 2016), pp. 221-247, page 240

footprints that are inevitably left behind. These digital footprints are can be constructed to build the individual we are and one cannot backlash at this juncture.

While Scott MnNealy, the chairman of Sun Microsystems, said in 1999 "You already have zero privacy anyway, get over it" and similar sentiments were expressed by Mark Zuckerberg who stated that Privacy is no longer the "social norm"[16] It is apparent that the internet and other late twentieth century developments have undermined the privacy of the individual, and at this position of trading privacy with efficiency, one cannot undo the comfort acquired with better services that the 'Internet of Things' has to offer.

It is trite that law has to adapt and amend itself to the new technologies, and it would be impossible to look at privacy merely through the eyes of Richard Posner.

Mark Zuckerberg prefers to work in the aquarium that is within a transparent glass cube in the middle of Facebook's headquarters at Menlo Park in California, which is 4, 30,000 sq.ft. And is the world's largest working space.

This is very similar to the zorbing ball analogy, where all of human activity is perpetually visible, but the only requirement is the lack of interference from such pursuit of activity. Within this ball, is one still left alone? And if not, the question still remains, to be left alone from what?

The human species is inevitably moving forward with greater dependence on technology. This cannot change and privacy at every step will only be a compromise. The Zorbing ball will have to succumb to multiple perforations and the exceptions to Privacy will loom large enough to consume the Right itself.

It is important for law to keep a check and the state to act in furtherance of the common good, as illustrated by the goals in the *Srikrishna Committee* report where India has taken the major step forward and is carving a niche in the Big Data World.

Acknowledgment

The author would like to thank her parents, brother and friends whose inputs have invariably contributed to the growth of knowledge in this field. In addition , subject teachers who have been a constant source of motivation and the immense knowledge they possess has always helped the author aim higher and strive for improvement.

REFERENCES

1. Robert Gellman and Pam Dixon, Online Privacy 'A Reference Handbook'
2. Daniel J Solove and Paul M. Schwartz, Information Privacy Law, 3 Ed.

[16] Online Privacy , Robert Gellman and Pam Dixon, page 15