UNDER COOKIES' COMMAND: SURVEILLANCE CAPITALISM AND THE RIGHT TO PRIVACY

- Vedanti Singhal*

Abstract

Author recently purchased winterwear from a well-established American brand and now my social media feed is swamped with woollen apparel ads. This happens due to 'surveillance capitalism,' a term coined by the scholar, Shoshan Zuboff. With the perks of digitization comes unwelcomed surveillance where users are used to commodify their data in a capitalist society. This paper attempt to elucidate on the concept of surveillance capitalism and the resultant, breach of privacy. For the sake of structure, this paper adopts a trace approach and discusses legislative initiatives and other company initiatives to uphold web privacy. In its last segment, a rather unheard solution is provided to ensure anonymity in dating sharing without impacting the end result.

Keywords: *Big Data, Surveillance, Marketing, Data Protection, Contextual*

* Student @ O.P. Jindal University; Email: vedanti_singhal@hotmail.com

INTRODUCTION

Big data refers to large, diverse sets of information that are constantly growing and its primary source is consumer's online activities.[1] By consolidating data, companies can optimize consumer demand, increase their product/service's efficiency in line with these demands and convert these consumers into prospective customers. Although analyzing big data for marketing purposes is not new, it does vest advertisers with powerful ways of understanding and predicting consumer preferences. Surveillance capitalism uses a business model based on big data for commercial purposes. *What is surveillance capitalism, then?* It can be understood as a market-driven process where the users' personal data is the commodity for sale.[2] This data is produced by mass surveillance of the internet carried out by big tech companies which provide free online services like search engines Google and other social media platforms.[3] In this process, the companies collect and scrutinise the user's online behaviour to condense the relevant data to create a marketing database. The Big Five, Google, Amazon, Facebook and Apple, collectively collate unmatchable quantities of data related to user behaviours, which they convert into products and services as explained in the following segment. More often than not, layperson is unaware of the extent of such surveillance. The process of data tracking and profiling is used in the form of surveillance capitalism to legally micro-target

[1] Saksham Malik, "Indian Merger Control Thresholds: effects of Recent Amendments on Digital Markets" Kluwer Competition Law Blog, *available at*: http://competitionlawblog.kluwercompetitionlaw.com/2022/01/10/indian-merger-control-thresholds-effects-of-recent-amendments-on-digital-markets/ (last visited on: 20.01.2023)

[2] Donell Holloway, "Explainer: what is surveillance capitalism and how does it shape out economy?" *The Conversation*, June 14, 2019

[3] Ibid

consumers, but this commercial incentive is resulting in a constant breach of right to privacy. This paper attempts to highlight the inept initiatives taken by companies and the guidelines issued by the EU while providing a potential solution.

CONTEXTUAL ADVERTISING: SOCIAL MEDIA EAVESDROPPING

The initial intent behind big data analysis was to reduce future uncertainties by predicting future behavioral patterns of data consumers. But now, the aim is to commercially monetize this data. The process of contextual surveillance is based on interlinked systems or "surveillant assemblages" of bureaucracies and social connection, embedded in our everyday lives.[4] There was an upshot of contextual advertising or behavioral advertising in 2000s with the launch of Google's AdSense where users would receive more personalized and relevant ads.[5] For instance, if X ran a food critic blog, AdSense might serve contextual ads like restaurant recommendations. As early as 2004, Google launched Gmail and acknowledged that it had scanned private correspondence for personal information.[6] This was

[4] Ian Brown, "The International Encyclopedia of Digital Communication and Society, Ch Social Media Surveillance", *available at:* https://onlinelibrary.wiley.com/doi/pdf/10.1002/9781118767771.wbiedcs122 (last visited on: 10.03.2023)

[5] Brian Platz, "New Digital Advertising is Rising from the Ashes of Surveillance Capitalism" *Forbes*, June 17, 2021, *available at:* https://www.forbes.com/sites/forbestechcouncil/2021/06/17/new-digital-advertising-is-rising-from-the-ashes-of-surveillance-capitalism/?sh=22a3a14556dc (last visited on: 10.03.2023)

[6] Joanna Kavenna, 'Shoshana Zuboff: "Surveillance Capitalism is an assault on human autonomy" *The Guardian*, October 4, 2019, *available at:* https://www.theguardian.com/books/2019/oct/04/shoshana-zuboff-surveillance-capitalism-assault-human-automomy-digital-privacy (last visited on: 12.01.2023)

supposedly a give-and-take relationship where users were served with relevant ads and companies would have a better grasp of users' tendencies. A widespread digital advertising industry grew around this model based cross-site third-party[7] cookie tracking. Users regularly disclose their personal information when they "accept all cookies" granting the site to track their online activities.

LOCATION-BASED MARKETING

Users of social media consider it to be an interactive platform meant for communication, sharing media and other information. But social media platforms use this information to create personalized profiles of individuals to later show them targeted ads.[8] WPP advertising company, for example, has built over 500 million personalized profiles globally.[9] To achieve greater precision in the consumption interest of the users, companies maintain a dossier of browsing information and analyse which potential interest matches.[10] This organisation, classification and sorting of collated data is called profiling. Targeting advertising is a practice of pairing viewers with advertisers on a real-time basis.[11] Profiling and targeting help in hyper-personalizing ads. Well received content is contextual, timely and relevant and pro-active and predictive marketing does exactly that.

With every swipe, tap, click on the screen, the user is tracked and targeted. Consider the following scenario where two people have a real-time

[7] Usually marketing companies external to the domain visited.
[8] Supra note 4
[9] Supra note 4
[10] Jiahong Chen, "Data Protection in the Age of Big Data" *Edinburgh Research Archive* (2018) *available at:* https://era.ed.ac.uk/handle/1842/33149?show=full (last visited on: 03.11.2022)
[11] Ibid

conversation regarding a product and an ad of that product pops up on their screen while scrolling Facebook. Many of these apps ascertain the user's geolocation based on GPS tracking and then sell this data to digital marketers.[12] Facebook and other social media platform surveil online behavior. So, in the abovementioned conversation, Facebook is privy to the knowledge that one of the friend's previously looked up that product on Google as it shadows the data trails he leaves, and by geo-location tracking it is aware that both the friends are together and thus, it targets the other friend with an ad of the same product. This is how websites compare interests based on the footprints. Geo-targeted mobile marketing is the fastest growing forms of advertising and one of the most controversial, instigating privacy advocates.[13]

The marketing industry persistently claims that targeted advertising based on behavioral data surveillance helps in serving internet users with interest-based tailored ads and enhance their overall online experience.[14] Contextual advertising is a business model based on persistent and invasive data collection. The problem arises when data is tracked not just to analyze and predict consumer behavior, but to change it. These companies wish to expropriate as much information as possible based on predictive algorithms and mathematical calculations to ensure certainty of user's future behaviour in order to intervene with it.[15] To alter future behaviour aimed at maximizing revenue, companies identify individual's behaviour of interest.

[12] Janella Nanos, "Every Step You Take: How Companies Use Geological Location to Target You" *The Boston Globe, available at:* https://apps.bostonglobe.com/business/graphics/2018/07/foot-traffic/ (last visited on: 10.01.2023)

[13] Ibid

[14] Supra note 10

[15] Supra note 6

Like E-commerce brands track not just individual's purchasing preference or behaviour but also see the time they spend on a product before making the decision to purchase in order to target special offers and influence purchasing patterns.[16] These predictive analytics helps marketers design advertisements to elicit unconscious and impulsive responses from its viewers.[17] This 'ubiquitous computing' has become a pervasive phenomenon that has faded in the backdrop of everyday lives where individuals unknowingly share detailed information.[18] Users allow companies to cash out their personal data because the enormity of surveillance is not that obvious to them. This has enabled expansion of data collection capacities since amount of personal data users share is unknown to them or has been normalized.

IMPACT OF SURVEILLANCE: PUPPETRY

Surveillance capitalism negatively impacts the individuals and the society, as a whole, thereby outweighing its benefits. It leaves humans as hackable entities and encroaches on individual autonomy and decision-making rights.[19] It dehumanizes people and sees them as objects evaluated in terms of how beneficial their response may be to their marketing strategies. Additionally, one is exposed to a "filter bubble"[20] where the internet is so personalized, tailored by tech-companies that it creates an impression the

[16] Supra note 4

[17] Comment on Petition for Rulemaking by Accountable Tech, *available at:* https://www.democraticmedia.org/sites/default/files/field/public-files/2022/childrens_coalition_survadv_1-26-22.pdf (last visited on: 10.01.2023)

[18] Supra note 4

[19] Amakiri Welekwe, 'What is surveillance capitalism and how can it affect you?' *CompariTech*, July 21, 2020, *available at:* https://www.comparitech.com/blog/vpn-privacy/surveillance-capitalism/ (last visited on:03.02.2023)

[20] Internet Activist Eli Pariser

internet is limited to their narrow self-interest.[21] An example of this bubble is personalized video recommendations on YouTube or even personalized feed on Facebook or Instagram. At face value, it may seem advantageous but in actuality, limited access to only personalized internet has the potential to undermine civil discourse and make users vulnerable to propaganda and manipulation.[22] This side of the internet could isolate individuals in their own cultural ideologies without attracting an educating or challenging dialogue. Since, data trails are permanently recorded, it confers unmatchable control to tech giants over its users. The subsequent consequence of this control is declaration. Online marketers simply declare its users' future.

Children and teenagers at the receiving end of online surveillance are more susceptible to its posited risks of behavioral and emotional manipulation. Young people consist of the significant audience of online experiences making them highly valuable for surveillance advertisers. Children are unaware that their personal data is commoditized to customize ads for them. Research suggests that children and teens are more easily influenced by advertising.[23] Commercial appeals to children makes it difficult for them distinguish between programming and advertising, facilitating the intended effects of targeted advertising. Unfettered exposure to marketing is the leading cause of health concerns in young children including childhood obesity,[24] substance abuse and dependence,[25] mental health issues,[26] and

[21] Ibid

[22] Supra note 19

[23] Report of the APA Task Force on Advertising and Children (2004) *available at:* https://www.apa.org/pi/families/resources/advertising-children.pdf (last visited on: 21.07.2023)

[24] Robinson, T. N., Banda, J. A., Hale L., Lu, A. S., Fleming-Milici, F., Calvert, S. L., Wartella, E, Screen media exposure and obesity in children and adolescents. *Pediatrics* (2017)

eating disorders among others.

Online surveillance also leverages insecurities of children against them. In 2014, in a memo drafted for advertisers, Facebook showed how they share psychological insights on its users, especially young people, with advertisers.[27] Facebook, by tracking its users' shared media in real-time, can recognize when they are feeling 'insecure' or 'need a boost of confidence.'[28] This was the largest known leak in Facebook's history. Alongside monitoring these emotions, Facebook can also identify how they fluctuate during the week. While youngsters, or people in general, are unloading their emotions online to seek support, Facebook is collecting these emotions and analyzing them to relay them to marketers. Even though Facebook claims that the emotional data aggregated was not used for any campaigns, sentiment analysis is not new on the internet.

The indiscriminate monitoring of personal data of adults and children alike is worrisome because children are not equipped to understand the process behind data mining and how it is used against them. In their formative years when children are impressionable, being exposed to online surveillance can potentially limit their opportunities. They are shown what marketers want

[25] Huang, J., Duan, Z., Kwok, J., Binns, S., Vera, L. E., Kim, Y., Szczypka, G., & Emery, S. L. (2019). Vaping versus JUULing: How the extraordinary growth and marketing of JUUL transformed the US retail e-cigarette market. *Tobacco Control*, *28*(2), 146-151 *available at:* https://doi.org/10.1136/tobaccocontrol-2018-054382 (last visited on: 12.02.2023).

[26] Report of the APA Task Force on the Sexualization of Girls, American Psychological Association (2007), *available at:* https://www.apa.org/pi/women/programs/girls/report (last visited on: 11.12.2023)

[27] Sam Levin, "Facebook told advertisers it can identify teens feeling 'insecure' and 'worthless'" *The Guardian*, May 1, 2017, *available at:* https://www.theguardian.com/technology/2017/may/01/facebook-advertising-data-insecure-teens (last visited on: 11.12.2023)

[28] Ibid

them to see. So, if the marketers have profiled and labelled children/teens as gamers or impulsive shoppers, they will be shown more related ads thus, tapering their interests and limiting their options of venturing out. Even if children and teens are able to recognize targeted advertisements, they are unable to resist them. This instinctive behaviour is not exclusive to young children. The movie, Social Dilemma, for instance, highlights how employees of these big tech companies, who are aware of the extent of surveillance, continue to fall prey to these manipulative techniques.

CAMBRIDGE ANALYTICA DATA THEFT: CAUTION LIGHT

Persistent and intrusive data collection was first recognized in the Cambridge Analytica scandal in 2018. Cambridge Analytica, a political consulting firm, worked for Trump's campaign and broke Facebook's own rules by collecting and on-selling private data of over 80 million users, under the pretence of academic research.[29] The data was acquired using a Facebook-based quiz which was a personality test. The data was used to grasp the users' political views and personality traits and they were then targeted with Trump campaigns. Facebook was fined for breach of privacy terms and Mark Zuckerberg was summoned before the US senate. Facebook faced worldwide backlash and criticism and users deleted their account. The hashtag #DeleteFacebook began trending on Twitter. To redeem itself, the company undertook some modest initiatives like a system of third-party fact checkers to ensure more transparency and opted for a policy to limit inauthentic coordinated behaviour. Cambridge Analytica's

[29] Nicholas Confessore, "Cambridge Analytica and Facebook: The Scandal and Fallout So Far" *New York Times,* April 4, 2018, *available at:* https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html (last visited on: 10.01.2023)

findings set way for the privacy awakening and ways in which data can be misused. In the following year, Mark Zuckerberg stated the need of an active role of the government and regulators for updating internet rules.

The scandal was a turning point which had significant implications on other tech giants. Apple recently launched App Tracking Transparency which gives its users the option of opting out of sharing their data with third-party marketing domains.[30] Later Safari blocked cookies by default and so did Mozilla in Firefox.[31] Google also claimed to limit cross-site tracking in Chrome by default by 2022.[32] However, Google has pushed the deadline to late 2024.[33] Some of these tech giants can offset revenue losses while others like Facebook, Twitter and third-party advertisers may face an economic burden. Like Google, despite limiting cross-site tracking in Chrome, can gather a lot of data through YouTube, Google Docs, Google Maps and other linked apps. Apple can also make up for losses through hardware sales.

PERSONALIZATION V. PRIVACY: LEGISLATIVE ROUTE

Social pressure coupled with the introduction of new regulations have posed challenges to the existing ad revenue model. In the backdrop of regulatory oversight and relational power dynamics between surveillance capitalists and internet users, Europe implemented the first rousing data privacy policy,

[30] Supra note 5
[31] Supra note 5
[32] Supra note 5
[33] "Google now delays blocking 3rd party cookies in Chrome to late 2024" *The Economic Times*, July 28, 2022; *available at:* https://economictimes.indiatimes.com/tech/technology/google-now-delays-blocking-3rd-party-cookies-in-chrome-to-late-2024/articleshow/93189036.cms?from=mdr (last visited on: 11.03.2023)

General Data Protection Regulation (GDPR), 2018. Although it is EU regulation, it also governs non-EU organizations that have offices in EU countries or that store and process data of EU users.[34] This means that the physical presence of a company in EU is not a pre-requisite for it fall under the scope of GDPR. GDPR is the latest legal response which affords paramountcy to individual privacy while curbing corporate commodification of personal data. It has set global standards pertaining to data collection, storage, and use.[35] The main of this policy is to enhance the control an individual has on their personal data and its dissemination. Provisions under GDPR lay down right to notification and require users to be informed how their data would be used and give them an option to opt out from giving their data.[36] It emphasizes on the importance of consent, given freely, before transmitting data to third-party marketers or those outside EU without prior agreement.[37] A distinctive and worth mentioning provision is the right to be forgotten. It says that any personal data stored by an online marketing domain must be erased as per the user's request, subject to certain conditions.[38] Throughout the legal framework, it is reinforced that an individual as an active agent in determining what is to be done with their data and it transgresses beyond mere passive "data protection." GDPR in some of its provision recognizes that data should not be used in any manner not permitted by its subjects, but, it fails to address the issues with data collection itself. So, a major shortcoming is that while it raises awareness

[34] Article 3, GDPR Territorial Scope of the Law

[35] Brett Aho & Roberta, "Beyond Surveillance Capitalism: Privacy, Regulation and Big Data in Europe and China" Taylor & Francis (2020), *available at:* https://www.tandfonline.com/doi/pdf/10.1080/03085147.2019.1690275 (last visited on: 11.01.2023)

[36] Article 13 & 14, General Data Protection Regulations

[37] Supra note 35

[38] Article 17, General Data Protection Regulations

amongst online consumers regarding data protection and violation of their privacy, it still neglects those that the policy was enacted to protect. This is not to undermine a major stride in the direction of combating privacy concerns in data collection. Since it is an EU specific regulation, other jurisdictions can inspiration to curate their own data protection policies.

MULTI-PARTY COMPUTATION: A PANACEA

A likely solution with an untapped potential to have a sweeping effect on the advertising technology data collection is Secure Multi-Party Computations ("MPC"). MPCs are procedures or a type of encryption that protects the security of private inputs.[39] It has been in existence since the 1980s but is only gaining prominence now. The search giant, Google, is already using this technology. Google Cloud has added a feature of Confidential Space which is based on this encryption where organizations get exclusive space to perform collaborative tasks without divulging private data.[40] In other words, MPC allows data sharing without leaving a trail of its origin. It uses blockchain technology where when one party enters data, it is broken down and encoded with numbers. The intended receiver of this data has to use a key to see it, which is decoupled from the user.[41] It is a zero-knowledge approach where the end result remains undisrupted. Advertisers can see all important data like how many people bought a product based on the new ad, or the number of rides shared during peak hours, but without

[39] Seung Geol Choi, "Secure Multi-Party Computation Minimizing Online Rounds" Springer (2009), *available at:* https://link.springer.com/chapter/10.1007/978-3-642-10366-7_16 (last visited on: 15.12.2022)

[40] Nancy Liu, "Google Cloud Creates Confidential Space for Multi-Party Computation" Sdx Central, Oct. 12, 2022, *available at:* https://www.sdxcentral.com/articles/news/google-cloud-creates-confidential-space-for-secure-multi-party-computation/2022/10/ (last visited on: 06.01.2023)

[41] Supra note 5

mining data in an invasive manner to affect individual's privacy. This enables statistical modeling and analysis without having access to the origin of the data.[42] MPC is a solid example of how technology evolves outside archaic business models with privacy consolidated in the process.

[42] Supra note 5