

# Surveillance Capitalism and Its Impacts on Data Privacy

Aditya Bhushan Sharma, Jaisraj Bhatnagar, Ishu Goel and Neelu Chaudhary

Computer Science & Technology  
Manav Rachna University  
Faridabad, Haryana – 121008

---

**Abstract**—This article discusses at length the most imperative topic that rules the world news today. We analyze the sensitive yet intriguing topic of Data Security. The primary analysis is to be carried on the free network sphere on the basis of the institutional practices and code of conducts followed by Google Inc. This method of accumulating large banks of data for the purpose of revenue creation and further third party usage is termed Surveillance Capitalism. Data Mining is fast increasing becoming a really impactful field of expertise with more and more of the real world gets digitalized. Hence computer-mediated transactions come into foray a lot more with data extraction, analysis, monitoring improvisations and continuous experiments for a better data gathering facet. Surveillance Capitalism depends on a computer mediation architecture on a global scale. This architecture constitutes various unexplainable processes of effective extraction, commodification, and control that lead to new predictions of general behavior. Hence Surveillance Capitalism works more on the past choices, decisions and actions of the people contradicting the centuries-old evolved system of Barter trade and market capitalism [1-2].

**Keywords:** Surveillance capitalism, data security, data mining, data privacy.

## 1. INTRODUCTION

The 21<sup>st</sup> century is a digital playbook. Wherein each and every person is accounted for. And by this, it does not mean just by certain general details that are necessary to be present in any kind of forms. It contains information that has that defines you, info that describes you. It's almost a virtual self. Hence any kind of surfing on retail websites, Web, E-commerce creates large amounts of data that is being profitably used by the corporations that control these architectures. And this conversion of our personal data that includes our preferences, temporal and spatial patterns and behaviors, hopes, dream and desires into a commodity which holds a certain value is broadly termed as under the strategy of Surveillance Capitalism. What is even more disturbing is the fact that all this data hoarding and commodification which eventually results in profit is done without any financial return to the user. Hence it is no more than a business where the user is sold is as a product to the markets wherein advantage is counted on the basis of targeted and user-specific product

development or provision. The use of Personal data in marketing is nothing new as it always been used for advertising and strategic marketing through general surveys which explored the preferences of a whole database of users to manufacture and further develop products [3].

However, a new dawn of personal data analysis has enlightened us which has been powered greatly by the advent of technology but also through o The 21<sup>st</sup> century is a digital playbook. Wherein each and every person is accounted for. And by this, it does not mean just by certain general details that are necessary to be present in any kind of forms. It contains information that has that defines you, info that describes you. It's almost a virtual self. Hence any kind of surfing on retail websites, Web, E-commerce creates large amounts of data that is being profitably used by the corporations that control these architectures. And this conversion of our personal data that includes our preferences, temporal and spatial patterns and behaviors, hopes, dream and desires into a commodity which holds a certain value is broadly termed as under the strategy of Surveillance Capitalism. What is even more disturbing is the fact that all this data hoarding and commodification which eventually results in profit is done without any financial return to the user. Hence it is no more than a business where the user is sold is as a product to the markets wherein advantage is counted on the basis of targeted and user-specific product development or provision. The use of Personal data in marketing is nothing new as it always been used for advertising and strategic marketing through general surveys which explored the preferences of a whole database of users to manufacture and further develop products [3].

However, a new dawn of personal data analysis has enlightened us which has been powered greatly by the advent of technology but also through our subjective approach of accumulation which we have come to know as Surveillance Capitalism [4].

Another worrying factor in the times to come would be the situation of power and credibility. Which will solely lie in the hands of a limited number of web corporations, Data dealers

and people who know how to fool this digital takeover. The increasing implementation of such personal data analytics techniques as a major economic strategy has caused a state of concern among several scholars of Data Privacy. They imply that social manipulation, data breach, and control are the major outcomes of the excessive application of Surveillance Capitalism on Data Privacy[4].

our subjective approach of accumulation which we have come to know as Surveillance Capitalism [4].

Another worrying factor in the times to come would be the situation of power and credibility. Which will solely lie in the hands of a limited number of web corporations, Data dealers and people who know how to fool this digital takeover. The increasing implementation of such personal data analytics techniques as a major economic strategy has caused a state of concern among several scholars of Data Privacy. They imply that social manipulation, data breach, and control are the major outcomes of the excessive application of Surveillance Capitalism on Data Privacy[4].

## 2. FACEBOOK & GOOGLE'S CAPITALISM MODEL IS IN TROUBLE

Privacy is a civil right that has been sometimes neglected by dataveillance. And since it becomes that much more important to protect it. You can't help but notice that Privacy as a socio- factor which gives you a foundation to achieve freedom of speech, action, and association. Without the fight for Privacy, it would become quite evident that users would become imminent victims of identity stealing while being under constant surveillance which might be a bit disturbing to endure [3,5].

People associate Facebook with their personal information, including photos and takes Google as a semi-reliable encyclopedia. But these services have only a tangential relationship to the way either company actually makes money. Both the Silicon Valley titans rely on two closely intertwined technologies, customer surveillance and advertising, to maximize shareholder profits. The pair controls 63 percent of the U.S digital advertising market, and in 2016, both secured 99 percent of all digital advertising growth [2].

Facebook sold companies on their platform by giving promising "brand awareness" and the best possible data on what customers liked. Brands are able to open their own Facebook pages and people can like it and can interact with. By engaging with companies on Facebook, people gave more corporate information than they could have ever dreamed of buying, but here it was offered up free. This is called "grand bargain" as Columbia University law professor Tim Wu called it in his book, The Attention Merchants [6].

In other words: We will give you every detail of our lives and you will get rich by selling that to advertisers.

## 3. METHODOLOGY OF SURVEILLANCE CAPITALISM

In this topic, we'll closely consider all the facets and features that make surveillance capitalism such an effective technique for modern-day data capitalists. This new method of data capitalism has made inroads into the Web-based industry and is making all the headlines with its new and effective tools of operation:

**3.1 Data Extraction And Analysis** – The first step in this working model of Surveillance Capitalism is the most obvious. It forms an expected and somewhat easy beginning to an otherwise complex architectural model. There are 2 main things that one needs to comprehend in order to grasp the crux of the particular aspect of surveillance capitalism.

Firstly, we need to understand and not undermine the sources that represent themselves as opportunities for data provision. By this, it means we have to look at the bigger picture and consider all the possible and anticipatory sources that may contribute to our objective of data extraction and mining. The most obvious source of data is the Web-based activities that each one of us undertakes in order to perform several different tasks. This analogy begs to retort to the previously confirmed observation of the 21<sup>st</sup> century to be a **digital playbook** wherein each and every Web-enabled transaction is logged and feed into a dataset so large and complex, that it is deemed far beyond the understanding capability of humans [1]. And these sources are increasing day by day as there is an exponential increase of smart devices (miniaturized as well as nanotech) that can be attached to every physical object if this world. Hence just think about the data value that any computers in future attached to your wristwatches, cars, thermostats and heck lawnmowers as well as washing machines would generate.

Secondly, we also need to take into account the relationship that Big data companies have with their prospective data buyers. This relation is solely based on Need to Know basis wherein the data is extracted and shared with buyers without the consent of the user. This data extraction process only comes to fray in the event of any data leaks that may lead to scams and revelation of ill practices [1-2].

**3.2 New Contractual Forms** – This aspect of Surveillance Capitalism is the most interesting of the lot and takes up a completely new form of data monitoring for discussion. Although a virtual concept till now but very much in the grasp of normal human implementation. This method of Contractual Monitoring as suggested by Chief Google Economist Hal Varian suggest that the presence of smart devices present in every stratum of human existence will lead to real-time monitoring and contract obedience to be deployed without the need of going to a court to enforce the terms of a contract and or terminate the same in case

of breach of terms. For example, if I don't walk 10,000 steps every day it might be possible that my health insurance company refuses to provide me with health cover owing to the data it collected through my smartwatch [1-2].

All this might be quite interesting and furthermore disturbing at times. But there is certainly a possibility of its implementation in the imminent future. Since there is not enough groundwork done earlier to corner these Big data companies into revealing their shady dealings of data, it becomes quite difficult to restrict their influence. There are generally quite a lot of social forces that desire this kind of system, as it brings with it power and unprecedented control over proceedings. But the society as a whole can only work upon the matter to free itself from this interwoven web of conspiracies [1].

- **Personalisation And Customisation Of Services** – The third structural aspect that works in tandem with the data extraction is the customization of the services that are analyzed and shortlisted on the basis of data (i.e., behavioral patterns, preferences of various kinds, etc.) for each and every user. This personalization in layman terms can be compared to a pact that is formed between doctor-patient, wherein one share highly personal information in exchange for benefits of personal service and advice. It is said that giving people the opportunity for exchanging their personal data in return for a better level of service provision will do nothing but improve their general standard of living.
  - All this said and done but there is strong mutual distrust that might arise from this comparison. Since in a doctor-patient relation, there is an emotional layer of interdependencies which arises from a feeling of trust and incoherence of the rule of law. Whereas the relation between Web-enabling companies that trade in big data to that of their users is nothing of this sort. It is in fact quite minimal in terms of trust endeavors as well there is no policy that enables application of rule of law. Therefore the user is unaware of the type and quantity of data that leaks to third-party vendors through these Web Enabling Companies [3].
- A. **Continual Experimentation-** Technological infrastructure do allow for continual experimentation into the lives of users. Using control groups we can easily test different digital services. This is because of the information collected from user profiles, geographical locations and so on. Some big examples can be. Facebook's attempt to manipulate the moods of its users is the most widely-known and discussed. Continual experimentation and intervention give rise to reality mining. By continual

experimentation, all the objects and events in the world can be manipulated by technological infrastructure [2-3].

#### 4. RECOMMENDATIONS & FUTURE REFERENCE:

What is Google's product we might think it is there map services, Gmail or search engine but they don't charge for anything above? Their product is the user and his data, companies like google, facebook, etc collects data from the free services you use and that data holds value. These online companies create a channel for the data between you and the advertisers. For example, Google will collect data from us and other users of similar interest then package you up to sell your data to the highest bidding companies.

Let's say in 2016 a company like Google made 80 billion dollars using the data of there users and they have around 4 billion active users. So on average that company earns on average 20 \$ from an individual's data.

In the real-world banking system, you gain interest when somebody else uses your money or property to earn profit but when it comes to our online data in the terms and conditions of the services we use we give away the rights to our own data for the services we are using. Which seems to be a fair deal but there can be a better way to do it. Let's suppose your data was not stored on the companies server instead it was stored in a literal data bank a government or an organization regulated institution where you store data then the data bank can lend out your data to corporations, government and other institutions which require such data to run their business in return to be allowed to do this the data bank pays you interest .Actually, the databank will not send out your data to the borrowers but only grant them indirect access, the borrower will send a data request to the data bank according to which the data bank will send only the end results to the borrower. This system will make the user more of a customer than a product. Over time this data bank system can also help the user generate lots of micropayments. In the making much healthier data-driven economy where everyone becomes an active participant.

Further technicalities of this data banking model are topic for future work and discussions

#### 5. CONCLUSION

To conclude there are four features of data surveillance capitalism.

- The first feature is growing and discovery of alternate data extraction methods and analysis.
- The second feature is the possibility of new forms of contractual monitoring and enforcement.
- The third feature is the desire to personalize and customize digital services.

- The fourth and final feature is the capacity for continual experimentation and intervention.

But we know from the multiple case studies like Facebook & Google, that attempts to manipulate the mood of the users or the attempt of a private company for manipulating voters that this pragmatic new method i.e., Surveillance Capitalism is not the healthiest way to execute data surveillance and there can be a better and healthier model which can be devised to overcome the issues of data privacy and unethical use of user data, one of such model we have lightly discussed in the proposal for future work and recommendations section. And we strongly believe there should be layer between user data and institutions that require them so that it can be monitored and violation of data privacy can be avoided.

#### REFERENCES:

- [1] Zuboff, Shoshana. "Big other: surveillance capitalism and the prospects of an information civilization." *Journal of Information Technology* 30.1 (2015): 75-89.
- [2] Cinnamon, Jonathan. "Social injustice in surveillance capitalism." (2017).
- [3] Clarke, Roger. "The digital persona and its application to data surveillance." *The information society* 10.2 (1994): 77-92.
- [4] Andrejevic, Mark, and Kelly Gates. "Big data surveillance: Introduction." *Surveillance & Society* 12.2 (2014): 185-196.
- [5] Lyon, David. "Surveillance as social sorting: computer codes and mobile bodies." *Surveillance as social sorting*. Routledge, 2005. 27-44.
- [6] John "The Logic of Surveillance capitalism".IEEE, futurism. 2015.