UNIVERSITY OF WESTMINSTER

7MEDS005W.1.2020

Political Economy of Communication

Academic Essay

The PEC of Digital Surveillance

Presented by **Jean Boutros** (W1804948)

Submitted on: Monday, 4 January 2021

Introduction

Every day, there are 1 million new internet users in the world. The Internet has already penetrated the lives of 4.3 billion people (Data Reportal, 2019). Presnky (2001) coined the word “digital natives” to refer to children being born into the digital age and mastering the use of technology without receiving any formal education on it. The Internet is now used for all sorts of transactions, whether social, political or economic. Platforms, apps, software, and phones have enabled a networked world but at the expense of people’s privacy. And while these platforms have been developed and sold under the pretext of connecting and informing people and enabling easier management of transactions, the benefits for corporations constantly and ongoingly collecting data on individuals through these platforms outweighs those of the users. Surveillance has become part of every person’s daily life with almost no means to escape it. Users have become enslaved by a capitalist system of surveillance that they have to take part of otherwise they could risk becoming marginalised, while the system is endlessly and increasingly generating profit from this model. This essay will discuss the political economy of surveillance and its implication on society. The essay will focus on the use of internet platforms as a medium of communication and its abuses as a form of economic surveillance. As such, I will limit surveillance to economic surveillance and practices of large internet media corporations.

Surveillance and data mining

Data mining is the process by which corporations collect, filter, and analyze data to predict potential risks or opportunities and constantly increase their accumulation of capital in

addition to controlling the crowds. Data mining can generate hypotheses or even with more advanced neural networks techniques, it can generate predictive algorithms (Ericson, & Haggerty,. 2006). It can take different forms and shapes but at the heart of it, it uses the internet and internet users to mine as much data as possible in one's lifetime. Data mining is a viable standalone business whereby data collected, compiled and sorted is sold to parties who have interest in the use of such data for an economic or political end. Some businesses even offer customization features when selling data. Large data mining companies like Aristotle, a leading political data-management software company, that claims on its website to have data on *"National Voter File containing 215+ million registered voters, National Consumer File of 245+ million consumer lists, National Donor File with 145+ million donations and a New Mover File refreshed with 1.2+ million new movers each month".* [1] This company sells customized data to their clients who are running for elections. They customize and sell data based on salary, age, location etc.. to better enable clients in targeting voters throughout their political campaigns. Another prominent use of data by other types of businesses is within the digital advertising space where data constitute the basis of the business models and income generation methods of these corporations. I will present this later in the essay.

[1] https://aristotle.com/political-data/

Some of the data mining tools used to collect data include “cookies”, or “tracking cookies”[2]. These help tracking people’s surfing habits and building accurate profiles of these people and their preferences. Cookies allow monitoring of every behaviour so long as the individual is connected. Nissenbaum (2010) makes a comparison of a day spent in a mall versus a day spent in the cyberspace, explaining that while an individual drives to a mall, scans shops and ultimately buys a scarf with his credit card which is the only recorded transaction on that date, online the same individual would be browsing through websites and platforms recording what caught his attention, what interests him, what his preferences are and how his decisions of purchase are made. (Confer & Heuple, 2017)

Generally, we can note 2 different purposes for data gathering by corporations: profiling individuals and risk assessment; and advertising as a business model.

Profiling and risk assessment

Data collected on individual’s behaviour online helps companies in profiling individuals to study the risk of giving them access to financial services such as loans or even insurances. (Ericson, & Haggerty,. 2006). However, the way they are used to generate findings is questionable. When analysing trends, data produces correlation rather than causation which could lead to the production of findings that are discriminatory. Confer & Heuple (2017) give the following example: if data from students of a class show that those seated in the back row averaged 20% lower on exams than those seated in the front row, the assumption is that

[2]https://www.cookiebot.com/en/tracking-cookies/#:~:text=Tracking%20cookies%20are%20cookies%2C%20i.e.,geographical%20location%2C%20and%20the%20like.

those seated in the back row perform less. In businesses, this can produce what is now called Web-lining, a term that is inspired by red-lining or racial discrimination, wherby corporations make discriminatory decisions on costs and quality of services offered to individuals based on data available from specific groups or individuals with a shared specificity in data (Ericson, & Haggerty,. 2006). In political contexts, this can also be detrimental to democracy. Choicepoint, a database company, sold credential verifications services to Florida's county board mistakenly identifying eight thousand African American voters as convicts. The same company is now emerging as the largest forensic lab in the US with a vision to add biometric data to their identity verification services. (Ericson, & Haggerty, 2006)

Advertising as a business model

When data is sold for advertisers it enables them to target the right clients with the right ads at the right time. The availability of this data not only enables corporations to enhance their profit but also reduce their costs. Data mining for advertising purposes is a business model of its own. Search engines like Google or social media platforms like Facebook constitute one of the biggest data mining tools existing. These 2 companies have a duopoly over the digital advertising space where they control two third of its revenues globally (Fresneda, 2018). Facebook has 1.8 billion active users worldwide[3]. There are 3.21 billion people actively using Facebook's apps each month. This includes Facebook, Instagram, WhatsApp and Messenger[4].

[3] https://www.statista.com/statistics/346167/facebook-global-dau/

[4] https://zephoria.com/top-15-valuable-facebook-statistics/

Over 2 billion people visit Youtube each month[5]. There are over 4 billion users for Google worldwide - this accounts for about 52% of the entire world population.[6] These platforms by nature have to collect data in order to function as business, survive, and be made available as a free app. It's their business model. Google for example has expanded its offering from search engine-only, to include free applications much needed in everyday life, with the aim of ultimately mining data on people's lives and preferences, which in turn would be sold to Google's advertisers. Fuchs (2012, a, p.33) spoke of a "Google's empire of economic surveillance" with strong economic incentives to introduce applications that serve the users in every circumstance from waiting for their bus to visiting family to spend more time online.

> *It is primarily economic surveillance i.e. collection, storage, assessment, commodification, of user data, user behaviour and user-generated data for economic purposes. (Fuchs, 2012a, p. 36)*

Behavioural data

Zuboff (2019) recalls in her book how Google started by using people's "behavioral data", which is data collected about individuals' behaviour online (website accessed, pages views, clicks, etc..) to improve its search engine results and ads. Previously, Google would base ads on user's search results, only for this to change and users' behavioural data to become necessary for "targeted" advertisement. Zuboff describes this as the "zero-cost asset" that creates surplus for a highly lucrative market exchange (Zuboff, 2019, p.82). This sort of

5 https://www.youtube.com/intl/en-GB/about/press/#:~:text=Over%202%20billion%20logged%2Din,in%20more%20than%20100%20countries.

6 https://review42.com/google-statistics-and-facts/#:~:text=Considering%20that%20there%20are%20almost,billion%20active%20users%20each%20month.

behavioural data is of high importance for online businesses like Amazon and Netflix. 75% of Netflix views are based on its recommendation which is the results of behavioural data. This recommendation engine saves Netflix 1 billion USD per year. [7] 35% of Amazon's purchases are through its recommendation engine. Youtube gets a 45% cut from any ad revenue[8].

Facebook is no different. In 2019, Facebook made 98.5% of its revenues from advertising, heavily reliant on behavioural data, rising from 4 billion in 2012 to 69 billion USD in 2019 (Clement, 2020). Moreover, the excess of "sharing" content or user-generated content provides Facebook with the legitimate tool to use and abuse users' data for economic ends. Users, under such platforms, have turned into commodities, having no right to object and being drawn into a system where they would be otherwise socially and potentially professionally excluded if they do not take part in it.

1.4. Data commodification and surplus accumulation: The surplus produced by the users whose data is being sold at immense economic returns helps capitalists accumulate even more capital. This surplus is partly produced by the companies' employees who are creating a platform appealing and engaging enough for the consumer to spend time on. However, in its majority, the surplus is created by the consumer himself, i.e. the user who is infinitely exploited by the platform collecting his data and generating income at the expense of his efforts and use of these platforms. Fuchs speaks of an "internet prosumer commodity", and here prosumer denotes the user who is the producer of the commodity as he engages in the

7 https://www.pointillist.com/blog/customer-behavior-data/

8 https://review42.com/youtube-statistics/

production of user-generated content, and its consumer at the same time. The Internet prosumer commodity therefore includes "user-generated content, transaction data, and the right to access virtual advertising space and time" transformed into a surplus and monetary capital. From a Marxist perspective, it's the labourer who is generating this surplus value (Fuchs, 2012b). Andrejevic (2001) compares this to the creation of factories where labour is controlled and monitored for the purpose of increasing productivity. This is what Andrejevic called "subsumption". In our modern world, labour, or users of these social media platforms and search engines who produce the value and surplus value through their usage, are subjected to panoptic surveillance where every behaviour is monitored and controlled and no information is missed and every opportunity is exploited. This information and constant surveillance according to Andrejevic is at the heart of productivity. Zuboff (2019) states that this behavioural surveillance that generates surplus and ultimately capital accumulation is "*understood as surveillance capitalism, which is the foundational framework for a surveillance-based economic order: a surveillance economy.* (Zuboff, 2019,p.93)

A global digital surveillance revenue

Using these models globally, these platforms under the pretext and connecting people and empowering them with information, have built a global empire where their power is concentrated in a market that makes it extremely difficult for any newcomer to enter and compete. As the table shows the global digital market space is dominated by these companies who control almost 80% of the total digital ad space, making it a moderately saturated market.

Company	*2019 Global digital ad revenue*	*Market share of global digital advertising (= 332.84 billion)*	*HHI*	*Overall revenues*	*Percentage of advertising revenue from overall company revenue*
Google	134.81 billion	134.81*100/332.85= **40.5%**	40.5*40.5= **1640**	160.74 billion	83.8%
Facebook	69.7 billion	69.7*100/332.85= **20.9%**	20.9*20.9= **436.81**	70.7 billion	98.5%
Alibaba		29.2*100/332.85= **8.7%**	8.7*8.7= **75.69**	71.99 billion	40,5%
Amazon	14.03 billion	14.03*100/332.85= **4.2%**	4.2*4.2= **17.64**	280.52 billon	5%
Baidu	15.00 billion	15.00*100/332.85= **4.50%**	4.5*4.5= **20.25**	15.43 billion	97%
Total		**261.93*100/332.85= 78%**	**2169.33**	**599.25 billion**	

This concentration of market power among these very few internet companies is worrying. Their overall market share in the global economy is worth almost 600 billion USD. This is equal to the total GDP of the 73 poorest countries in the world together, meaning only these 5 companies generate more income than 73 countries combined. (Based on calculations of GDP data from the World Bank, 2020). Moreover, in the table I show how these companies rely on advertising to generate billions in revenues. Their continued domination over the consumer or user is key to their survival, while in a capitalist world, their economic weight leverages this power.

A threat to democracy and to human autonomy

Needless to say, the scandal of Cambridge Analytica, the data mining company that worked for the Trump and Brexit campaign, has proved how abuses of data are threatening democracy. Fuchs in an interview spoke of a "dangerous triple alliance": digital capitalism, neoliberal ideology and extreme right" (Fresneda, 2018). More than just selling data during elections, data is being sold to governments. Snowden's leak of big tech companies like Microsoft, Apple, Facebook, Yahoo and Google selling data to governments under the PRISM project came as a shock to the entire world and until today governments are silencing Snowden. The same tech companies were not able to reveal their involvement in the "bulk data'' collection and mass surveillance project as they were prevented by a court order. The same practice is taking place in China but less secretively, as Fuchs (2015) notes, under the pretext of "information security management". Ma Huateng the CEO of Tencent affirms in an interview question that they "are a great supporter of the government in terms of the information security." (Fuchs, 2015). This complicity itself is a threat to individual freedom and participation (Zwart, Humphreys, & Dissel, 2014, Zuboff, 2019, p. 361), an ideology that Fuchs argues that it is deprived of its political meaning and is only presented by the West and China as a mere illusion to deflect attention from the "political-economic control structures that fuse authoritarian politics and neoliberal capitalism" (*ibid.)*. The practice of mass surveillance, nevertheless, remains a deterring factor to freedom of speech and public participation, two key enablers of Western democracy and Eastern autonomy and individual

freedom. For this reason, surveillance should be accountable and should undergo some sort of regulation that guarantees the future of netizen's participation.

Regulating surveillance capitalism: Neoliberal and social theory of privacy

When we discuss surveillance and its political economy, it is equally important to discuss privacy and regulating the internet space. Privacy is a fundamental human right protected by Article 8 of the Human Rights Acts. However, digital rights have sipped through the holes with the technological development of digital platforms which required governments to rethink the protection of their citizens in the modern world and provide more focus on the use and processing of data (Hoofnagle van der Sloot, & Borgesius, 2019). Since 1990, draft directives have been suggested and adopted by the European parliament and the council of 24 October 1995 to regulate the processing of personal data (EUR-Lex, 1995)[9]. Different iterations of these directives and earlier law - the Data Protection Directive - have led to the development of what we know now as the GDPR, the European Union's General Data Protection Regulation proposed in 2015, adopted in 2016 and fully enforced in 2018. Previous directives had a certain extent of data protection however, were criticised for their lack of enforcement. The GDPR offered more protection and further rights to data subjects and more burden to third party data processors and created privacy regulators in 30 European countries who are supposed to have the role of enforcing the law. (Hoofnagle van der Sloot, & Borgesius, 2019). Yet, the GDPR itself was criticised for its lack of enforcement. Regulators are understaffed and

[9] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

under resourced. Luxembourg whose role was to regulate Amazon, had a budget for €5.7 million in 2019, or roughly Amazon's sales over 10 minutes. Ireland is responsible for regulating Google, Facebook, Linkedin and Twitter, yet with a budget of €16 million a year. Since GDPR came into place, Ireland didn't issue any penalty. (Satariano, 2020).

More than just practical challenges to application of the GDPR, it also faces existential challenges. GDPR has ensured people's right to privacy are respected by organisations using their data, but we must also ask the question whether it has ensured that people do not lose privacy when they willingly submit their data for use by these companies and citizen's interest and wellbeing is still ensured. Nowadays with GDPR, people have to agree on how their data is collected prior to browsing a website, and can also manipulate their privacy settings more easily on renowned platforms. However, how exactly their data is used and by whom and for what purposes remains cryptic and impossible to understand by an average user. Scholars have proposed a socialist approach to privacy where instead of protecting individual's rights, the policy would seek to protect the abused consumer from the dominant corporation. It assumes an asymmetry in knowledge between corporation and consumer and makes an emphasis on the need to shy away from a liberal theory of privacy that treats consumer and corporation equally. Instead the social theory of privacy posits that they should not be treated equally because not both have an equal economic and political power. Increasing the protection of consumer's privacy would be economically advantageous to the consumer who may be for example less bombarded by targeted ads and less inclined to spend his income entirely but could be economically disadvantageous to corporations who no longer can

produce a surplus. However, the social theory of privacy does not aim to protect corporations nor their surplus which it considers an abuse in the first place. Also, it argues that treating both consumer and corporation equally means that corporations have equal right to conceal information that is important for the consumer, but when concealed, could help them engage in this abusive power behaviour. (Confer & Heute, 2017).

Conclusion

Surveillance and data importance in the digital capitalism realm is not going to change and data will not decrease in importance. Large corporations will always find ways to circumvent the laws or use their power to influence policy and decision making. GDPR has been a right step towards an increased protection, however, more needs to be done to protect the users. More than just fixing the capitalist digital space, we can look at an alternative public service internet as proposed by Fuchs (2017) to strengthen the public sphere which is much needed for society's critical capacities.

References

Clement (2020). Digital advertising revenue of leading online companies 2012-2019. Statista. Feb 7, 2020. Available from https://www.statista.com/statistics/205352/digital-advertising-revenue-of-leading-online-companies/

Confer, S., & Heuple, K. (2017). A socialist theory of privacy in the internet age: An interdisciplinary analysis. *Philologia*, *9*.

Creamer-Flood (2020). Global Digital Ad Spending Update Q2 2020. E-Marketer. July 06, 2020. https://www.emarketer.com/content/global-digital-ad-spending-update-q2-2020

Data Reportal (2019). Digital 2019, Global digital overview. 31 January 2019. Available at https://datareportal.com/reports/digital-2019-global-digital-overview. [Accessed 09 December 2020]

Fresneda (2018). Christian Fuchs: "We have to change the networks to save democracy". El Mundo, June 05, 2018. Available from

https://www.elmundo.es/television/2018/06/05/5b1589de22601d84308b45ec.html

Fuchs, C. (2012,a). The political economy of privacy on Facebook. Television & New Media, 13(2), 139-159.

Fuchs, C. (2012,b). Critique of the political economy of web 2.0 surveillance. *Internet and surveillance. The challenges of web 2.0 and social media*, 31-70.

Fuchs, C. (2015). *Culture and Economy in the Age of Social Media.* Routledge.

Fuchs, C. (2017). Towards the public service internet as alternative to the commercial internet. ORF Texte, 20, 43-50.

Hoofnagle, C. J., van der Sloot, B., & Borgesius, F. Z. (2019). The European Union general data protection regulation: what it is and what it means. *Information & Communications Technology Law*, *28*(1), 65-98.

Ericson, R. V., & Haggerty, K. D. (Eds.). (2006). *The new politics of surveillance and visibility*. University of Toronto Press.

Prensky, M. (2001). Digital natives, digital immigrants. *On the horizon*, *9*(5).

Satariano, A. (2020). Europe's Privacy Law Hasn't Shown Its Teeth, Frustrating Advocates. The New York Times. 27 April,2020. Available at https://www.nytimes.com/2020/04/27/technology/GDPR-privacy-law-europe.html

Wahl-Jorgensen, K., Bennett, L., & Taylor, G. (2017). The normalization of surveillance and the invisibility of digital citizenship: Media debates after the Snowden revelations. *International Journal of Communication*, *11*, 740-762.

World Bank (2020). World Development Indicators. Databank. Available at https://databank.worldbank.org/reports.aspx?source=2&series=NY.GDP.MKTP.CD,NV.AGR.TOTL.ZS,NV.IND.TOTL.ZS,NV.IND.MANF.ZS,NV.SRV.TETC.ZS,NV.SRV.TOTL.ZS#

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power: Barack Obama's Books of 2019*. Profile Books.

Zwart, M. D., Humphreys, S., & Dissel, B. V. (2014). Surveillance, big data and democracy: Lessons for Australia from the US and UK. *UNSWLJ*, *37*, 713.