Communication and Culture Review
Vol. 1, No.1, 38-49

The biopolitics of privacy in MalluApps and Pandacat: An analysis of third party fun apps in Facebook

M. Shuaib Mohamed Haneef, PhD

Rajeesh Kumar T V

ABSTRACT

There is a glut of ethical concerns, emergent and generative, involving Facebook and third party applications within Facebook. This paper seeks to explore the potential ethical and privacy concerns of third party applications deployed in Facebook by analysing two popular applications namely www.malluapps.net (in Indian native languages) and www.pandacat.me . By carrying out an analysis of the privacy statements of the two applications, the paper examines how privacy concerns are articulated in terms of users' privacy, liability, information transfer and sharing. The privacy concerns arising out of the analysis has been examined through Helen Nissenbaum's (2010) normative privacy model of 'contextual integrity'. Further, the paper seeks to explore how users, through the regime of biopolitics, get exploited and cede themselves and their privacy to the owners of the two applications.

Keywords: Privacy, contextual integrity, third party applications, biopolitics, www.malluapps.net, www.pandacat.me

M Shuaib Mohamed Haneef, Ph.D. is Assistant Professor in the Department of Electronic Media and Mass Communication, Pondicherry University, India. His areas of interest include digital media and culture studies, interactivity and agency, convergence practices, digital media and affect studies and game studies.

Rajeesh Kumar T V is a Junior Research Fellow at the Department of Electronic Media and Mass Communication, Pondicherry University. He was earlier working as Research Fellow Project Fellow for a UGC Major Research Project titled "Social Media and Ethics: A socio-technical approach to the making of ethics among children and youth of Pondicherry and Tamil Nadu". His research interests include new media studies, political economy of media and political communication.

Introduction

Social Networking Sites (SNS) are widely endorsed as the nerve centre of the Web 2.0 era owing to the fact that they enable a new, vibrant, user-centric and interactive environment. Facebook, as one of the most popular social networking sites in the world, has given rise to discourses on network culture, networked individualism (Wellman, B et al., 2006), neoliberal subjectivities especially predicated upon what it strives to achieve through its commercial activities.

Privacy has been a controversial subject pertaining to the activities of Facebook ever since it became a noticeable networking platform. Relatively lethargic approach of the platform owners has many a times attracted stringent criticism. In 2010 itself Mark Zuckerberg has apparently stated that the age of privacy is over (Kirkpatrick, 2010). In recent times Facebook has attracted mounting criticism over data breach and compromising on the privacy of users. The recent Cambridge Analytica controversy, which has galvanised worldwide discussion pertaining to online privacy, opens up discourses on privacy policies and digital media ethics.

The ethical concerns surrounding the use of data generated by users and feigning of privacy at the cost of putting the data out in the common space point out how Facebook could possibly exploit 'labour' and leisure (Scholz, 2013). Facebook lays out several terms and policies germane to the privacy of users where it states that data generated on the platform will be accessed and utilized by the developers. Similarly, it provides opportunity for the third parties to develop different applications which can be used to access data and eventually dump targeted advertisements on users' news feeds. Corollary to Facebook being able to access user data, it generated 9.16 U S dollars revenue from advertisements in the second quarter of 2017 (Swan, 2017).

The third party applications hosted in Facebook also pose ethical and privacy issues as they exploit the leisure time of users to engage in digital labour and thus towards capital accumulation and intensification of capitalistic social regime. This paper attempts to examine privacy issues that third party fun applications namely MalluApps and Pandacat hosted in Facebook can give rise to in the Indian context.

To understand the impinging privacy threats related to these applications, the authors carried out an analysis of the privacy policies of both these applications. Further, the paper analyse privacy using Nissenbaum's (2010) concept of 'contextual integrity'. This paper also seeks to explain the digital labour distribution in third party fun applications and its exploitive dimensions from the theoretical frameworks of biopolitics, digital labour and unwaged immaterial labour.

Privacy in Indian Context: The Conundrum

The Right to Privacy is not guaranteed as an explicit right in the Indian Constitution. Instead, Article 21 of the Constitution, which guarantees right to life and liberty, is interpreted and read as an encompassing right that extends to the right to privacy. The recent Supreme Court verdict ((K S Puttaswamy v Union of India, 2017) underlines the fact that right to privacy is intrinsic in Article 21 of the constitution. Concluding the verdict of the case between Justice K S Puttaswamy and Union of India, on 24 August 2017, the apex court made it clear that "the right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the constitution" (K S Puttaswamy v Union of India, 2017).

As a fundamental right, it is incumbent on the State to guarantee the right to privacy to its citizens. But, on many occasions, the government argued that the right to privacy is not a constitutional liability and that the government is under no obligation to guarantee it. The dialectic between the judiciary's insight and the State's repudiation of the right to privacy has reached a flashpoint in the Indian context. The Supreme Court of India recently staved off the State's order to link Aadhaar card to bank accounts (G Ananthakrishnan, 2018). On the other hand, the Law Ministry of India states that there is no attempt to meddle with individual privacy and legitimizes the need for linking Aadhaar to citizens' bank account, mobile phones and welfare schemes (K. Rajagopal, 2017).

Even as differences exist, the discourse on making the right to privacy as a standalone act in the Indian Constitution has been very active in the country following the mounting new challenges and concerns posed by raging technological advancement. In its judgement on Puttaswamy vs Union of India case, the Supreme Court said,

> 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. (K S Puttaswamy v Union of India, 2017, P. 4-5).

Technology, Data Protection and Online Privacy in Indian Context

The Information Technology Act of 2000 (IT Act), has addressed, though inadequately, some of the major issues that have emerged after the arrival of internet technologies. For instance, the successive governments tried to enhance the ambit of the IT Act by making necessary amendments to it from time to time. In 2008, Section 43A was inserted into the IT Act to address the issues of personal data mining and protection of the mined personal data. This section elucidates how the corporate and other business organisations are liable to ensure protection of the personal data of their customers and any negligence in this regard is punishable with compensatory payment. The section also lays down a condition that demands that consumers be informed about how their personal data will be shared and used by companies before accessing their personal information. In 2011, Section 43 A was further enriched with the introduction of eight additional rules that define personal data, extent to whom personal data about consumers can be transferred and the period it can be retained by the corporate.

Yet, the growing concerns stemming especially from social networking sites have compounded privacy issues making the IT Act ineffective. The Act, in particular, was seen insufficient to address covert data mining by private and government agencies. Further, the ambiguity of some sections in the IT Act lent itself to criticisms and scrutiny. On March 23, 2015, the Supreme Court of India struck down Section 66 A of the IT Act observing that it breaches a citizen's right to freedom of speech and expression. The apex court said, "Every expression used is nebulous in meaning. What may be offensive to one may not be offensive to another. What may cause annoyance or inconvenience to one may not cause annoyance or inconvenience to another" (J Sriram, 2015).

Realising the inadequacy of the IT Act of 2000 in addressing personal privacy and data protection, a special group comprising several legal and policy experts was formed by the Indian government in 2010 to bring out a strong privacy framework and address the complicated aspects

of privacy protection. After holding several discussions within the committee and deliberations with civil organizations, local practitioners, banking and business representatives, the special group submitted an 'approach paper' to the government to evolve a legal framework on privacy.

Addressing the question of the need for privacy protection, the 'approach paper' perceived that India did not have a general data protection statute. It further observed that though the right to privacy is guaranteed under Article 21 of the Constitution, almost all cases pertaining to privacy were handled in the context of the government's abjuration of the right to privacy to its citizens. The absence of a reassuring judicial precedent granting citizens a right of action against the breach of privacy on him/her was considered vacuous and the committee observed that the privacy jurisprudence in India had not yet fully matured.

Discussing and forecasting the privacy issues of the future, the special group expressed their concerns on the gloomy threats that Unique Identification Number alias Aadhaar could cause to the privacy of individuals. The committee opined, "Such a vast interlinked public information database is unprecedented in India. It is imperative that appropriate steps be taken to protect personal data". (Approach paper for legislation on privacy, 2010).

Based on the proposal of the special group, the Indian government came up with two major bills namely the Privacy Protection Bill, 2013 and Personal Data Protection Bill 2014 to deal with privacy protection and personal data protection. But, both these bills have been kept in abeyance and uncertainty continues to prevail as to when they will be made into laws. Though the approach committee's proposal was endorsed and drafted as two major bills, the lacklustre approach in implementing a new privacy law suggests that the government's motive to introduce it is fraught with contradictions and controversies. The Privacy Protection Bill, 2013 and Personal Data Protection Bill 2014 are yet to be passed by the parliament and thus the implications of these bills in the day to day issues are merely hypothetical.

When discussions on implementing the two bills were brought up in the Rajyasabha on May 4, 2016, the Information and Technology Minister responded that the Government of India is still drafting a comprehensive privacy bill and a timeline for the implementation could not be given (Pai, V, 2016, www.medianama.com). Against the backdrop of inadequate legal framework, this study seeks to explore the implications of third party applications in Facebook for data protection and privacy.

Immaterial Labour and Bipolitics

Exploring the changes in the working atmosphere, labour, and power relations in accordance with the introduction of new technologies, Lazzarato (1996) elucidates two aspects of "immaterial labour" which is exploited by the bourgeoisie (Lazzarato,M, 2004, P. 187) .

Lazzarato (1996) expresses immaterial labour along the axes of technical skills and the subjective agency of the working class. The immaterial labour, which involves use of computers, cybernetics and technologies and further captures changing labour practices due to new developments, produces 'informational content' of the commodity. On the other hand, the immaterial labour, which does not refer to work, but involves defining fashions, tastes or moulding public opinion, produces 'cultural content' of the commodity. Lazzarato (1996) argues that in digital ecosystem the management wants the personality and subjectivity of workers to become susceptible to its will and orders.

Hardt and Negri (2006) argue immaterial labour as biopolitical in that it is oriented towards the creation of forms of social life. Such labour, then, tends no longer to be limited to the economic but also becomes immediately a social, cultural and political force. Supplementing Lazzarato's

notion of immaterial labour, Hardt and Negri (2000) discuss a third type of immaterial labour which involves the production of affect, i.e., affective immaterial labour. Hardt and Negri (2000) draw the idea of immaterial affective labour from the concept of 'women's work', which was deliberated by the feminist thinkers. "Caring labour is certainly entirely immersed in the corporeal, the somatic, but the affects it produces are nonetheless immaterial. What affective labour produces are social networks, forms of community, and biopower". (Hardt and Negri, 2000, p. 293)

Hardt and Negri (2000) quote examples of health services and entertainment industry to delineate affective labour by underlining its products that are marked by feelings of ease, satisfaction, excitement, or passion. Extending similar notions, Terranova (2000), Cote and Pybus (2007) use the term immaterial labour 2.0 to explain the labour taking place in digital platforms.

> Brown (2007) terms the labour on digital platforms as unwaged affective labour. Brown (2007) puts it as,
>
> the term unwaged affective labour better emphasizes the intimacy that obtains between the unwaged producer of immaterial artifacts and the artifacts themselves at the same time as it foregrounds the social relationships and network prerequisite to this kind of work. (Brown, 2007, p. 8)

Brown (2007) elucidates on the concept of unwaged affective labour and explains how the user labour is exploited by platform developers making an illusion of common that is indeed a quasi-common. He uses the term quasi-common to explain how users and owners hold contradictory notions about a single platform. Brown (2007) argues that the social networking platform developers see websites as a means to make more and more profit whereas the unwaged affective labourers of these sites beaver away to seek pleasure, ease and enjoyment by communicating their thoughts and interacting with others. In other words, these affective labourers are devoting their time to indulge in networking activities to gain something more valuable than the money which is apparently contradictory to the thoughts of platform developers. Brown (2007) perceives this exploitation as potentially biopolitical and explains that by aggregating, analysing, interpreting and selling the data created on the platform, social networking sites and services are creating concentrated and valuable audience commodity.

Facebook, Leisure and Labour

Smythe (1977) has proposed the concept of audience commodity to explain the working mode of advertisement-driven mass media. Audience as a commodity was less explained till that period and was very much over looked by the western Marxist media thinkers. Pointing to the nexus between mass media and advertisers, Smythe (1978) argues that the actual commodity form of advertisement-driven mass media in the monopoly capitalism is nothing other than the audience or readership. Smythe (1978) explains, "Audience and readership are the workers of commercial media. They create the demand for the advertised goods and by consuming media, they reproduce their own labour power" (Smyth, 1978, p. 465). With Smythe's arguments as the base for further research works, many thinkers have come to delineate the new form of exploitation in digital space.

Unlike traditional business organizations, concerns over how SNSs make money and what are the products they sell in the market are scantily discussed among users (Tippet, 2015). According to Tippet (2015), Facebook exploits its users' labour in three ways to produce commodities; enrolling more users, collecting their personal data and selling these data to

advertisers. Tippet (2015) argues that millions of users indeed actualise a business venture like Facebook. Without users and their contents, Facebook would be meaningless and eventually valueless. The accumulation of users' personal information in pursuit of profile creation is the second aspect which is exposed to exploitation. Facebook collects the individual's name, email address, origin, religion, phone number, political orientation and other such cultural and social information. Facebook sells these private details to advertisers and ultimately advertisers use these information to cultivate consumer interest among the users of Facebook (Tippet, 2015).

Holding the base of the analysis on the Marxian theory of value, and correlating Smyth's (1977) concept of audience commodity to the Web.2.0 era, Fuchs (2013) explains how the users of Web 2.0 based SNS are being exploited by platform developers or capital investors. Explaining users as the life blood of social networking sites, Fuchs (2013) explains, as in the audience commodity, the user generated contents and data, which are very much the labour of the users of these platforms, are simultaneously sold to advertisers and exploited by platform developers. On Facebook, users create and reproduce contents that include personal data, social connections, communications and communities. Indeed all activities on Facebook are stored, assessed and commodified (Fuchs, 2013). He compares content generation to the process of production and the data produced to the commodities that are sold in the market. Basically all the data that are created on the social networking platforms are the outcome of the users' labour. Drawing attention on the capital accumulation strategies of social networking sites, Fuchs (2013) substantiate that all these sites are driven by the capitalistic mode of time organisation. In this scenario, Fuchs (2013) argues that in social networking sites the user labour is exploited in such a way that the user does not feel it like physical labour, rather the labour time is extended to leisure time and leisure time turns into labour time.

Shedding light on almost similar notion of exploitation that takes place in Social Networking Sites, Terranova (2000) has discussed about 'free labour' which is being exploited in social networking sites and explained free labour as "simultaneously voluntarily given, unwaged, enjoyed and exploited". (Terranova, 2000, p.2). Both Fuchs (2013) and Terranova (2000) focus on the exploitative dimensions of labour taking place in the digital space and speak less about the exploitative nature of social media spaces.

Third Party Fun Applications on Facebook

Facebook has been a vital concern of international privacy discussions and arguments ever since the company catapulted to the reputation of a global social networking giant. As the company came up with new modifications on its architecture and working features, the privacy apprehensions also increased among the users. The seminal privacy concerns on Facebook were the inappropriate use of personal information and the undesired flow and sharing of information to others. The hosting of third party applications in Facebook further compounded privacy concerns among users.

Facebook allows its users to maintain a developer account through which one can host third party applications utilising Facebook's Application Programming Interface (API). These third party applications arguably serve to enhance the social experience on Facebook and supposedly fulfil the entertainment needs of its users. Many of these third party applications on Facebook are also fun-based allowing users to play games, find answers to unexplored questions and to forecast future events. Though the services of third party fun applications are said to be free of cost, these apps appropriate more valuable private details and personal data of users in the guise of fun and entertainment.

Heather Lipford et.al (2009) in their study on design of privacy mechanisms on SNS, argue that the users of third applications are not adequately aware of what they are sharing with these applications and they are least known about the developers of such apps. Although privacy policies are notified on the platform, merely a few users would spend time to understand them. In another study of Facebook's partnership with third party apps, Hashemi (2009) found that the platform has made a shift in its advertising model in order to augment profit. According to Hashemi (2009), the new advertisement strategy of Facebook is twofold where on one hand the company started pumping in advertisements to a user's friends and on the other hand Facebook tracks user's activities on third party applications and eventually delivering advertisements on the basis of activities and patterns captured.

Methodology

This paper seeks to engage in a discursive action pertaining to privacy implications of third applications in Facebook by analysing two applications namely MalluApps and Pandacat with focus on the Indian context and tries to answer the following research questions. In this paper, the authors have chosen two popular third party fun applications in Facebook namely MalluApps and Pandacat for the study. These applications are widely used by Indian Facebook users for fun and entertainment. While Pandacat serves a broad population of English users, MalluApps caters exclusively to Tamil and Malayalam speaking Facebook users. These apps help the users in finding out answers for some hypothetical questions such as how much users love their dogs, which friend balances their personality, who is their second self, who is their soul twin, and who are their true friends among others. The answers to these hypothetical questions are generated on the basis of users' Facebook activities and their friends' reactions on their timeline. Though privacy policies of MalluApps and Pandacat are presented in brief and lengthy formats respectively, both are focused on providing fun and leisure. As a method of enquiry, an analysis of the privacy policies of these applications are carried out against the backdrop of Helen Nissenbaum's theory of contextual integrity. Further this paper seeks to explore the biopolitics of privacy in third party applications.

According to Foucault (1976) biopolitics is a mechanism or strategy that are used by the regime of authority in the process of subjectivation, knowledge and power. Foucault explains, "biopolitics deals with the population, with the population as a political problem, as a problem that is at once scientific and political, as a biological problem and as power's problem". (Foucault, 1976, p. 252). In this study, the researchers try to locate privacy and users' data as a biopolitical tool in creating a homogenous subjectivity that strengthen the neoliberal regime of authority.

Nissenbaum (2010) has argued that existing privacy framework does not adequately describe phenomena such as public surveillance, consumer profiling, and data mining Nissenbaum (2010) has analysed privacy in context and explains that there is no such thing as context free information or universal privacy norms. Instead, she conceptualises a new privacy framework – contextual integrity – where privacy can be grounded on two norms of information flow namely 'norms of appropriateness' and 'norms of distribution'.

While 'norms of appropriateness' explain "what information about a person is appropriate or fitting to reveal in a particular context (a professor may be highly visible to other gays at the gay bar but discrete about sexual orientation at the university)", 'norms of distribution' deals with whether information about a person can be transferred and if so with whom (friends expect what they say to each other to be held in confidence and not arbitrarily spread to others".) Hence, the

privacy expectations of Nissenbaum are about endorsement of both 'norms of appropriateness' and 'norms of distribution'. If any of these norms is violated, it can be understood as the breach of contextual integrity. Drawing on these theories, this paper seeks to answer following research questions.

1. What are the privacy discourses discussed in the privacy policies of MalluApps and Pandacat?
2. What are the implications of Nissenbaum's contextual integrity privacy approach in understanding the privacy policies of MalluApps and Pandacat?
3. In what ways do the third party applications MalluApps and Pandacat use the privacy of the users as a biopolitical tool?

Privacy Policies and Liability of Privacy

Third party applications and Facebook are apparently two different commercial entities. One of the clauses in the privacy policies of MalluApps states:

> This application is not the part of the company Facebook/ Facbook.inc. This application uses Facebook API to get your necessary information and work as you use. (Terms & Condition, retrieved from: https://malluapps.net)

This clause indirectly attributes the liability of data distribution to Facebook as it categorically states that content offering by MalluApps depends on Facebook API to get necessary information and data of the users. The Data Protection Bill of India does not clarify its implications for third party applications hosting their content in social media hosting platforms. Invariably, Facebook and its APIs in this context, on account of having control over the content of third party applications, allow its developers to operate its servers in a nodal server.

The major privacy concern arising out of third party applications in social media is that of data mining or data distribution for targeted advertisements. The privacy policies of MalluApps require the user to log into the application only by giving away his/her basic account information, wall posts and inbox details. The application Pandacatalso gathers almost similar data from the user. The basic question that emerges out of this is whether this data mining is lawful or not?

Though data mining and data distribution are punishable under the Data Protection Bill of India, the same may not construe a criminal activity if prior consent is obtained from users. As far as MalluApps and Pandacat are concerned, if one has to indulge in entertainment activities in these applications, the user consent for giving away personal data is mandatory. Hence, an active user of these applications is one who has already given the consent to a third party to use his/her data.

Once the consent for grabbing personal data is granted to third party applications, the consequences of every action performed on the social networking site concerned become the liability of the user. While MalluApps makes the user liable with a word of caution stating "your use of any information or materials on this application is entirely at your risk, for which we shall not be liable", the statements of Pandacat are in a sense presupposed and obfuscating when it reads "we collect and process your personal data within the scope of your registration and the service".

Though these two applications escape the ambit of the expectations of Personal Data Protection Bill of India, it can be analysed against the privacy frameworks of privacy experts. One such privacy framework and discourse this study uses to foreground its arguments is contextual integrity postulated by Nissenbaum (2010).

Privacy, Contextual integrity and Third Party Applications

According to the privacy policies of Pandacat, to be able to log in to the app, the user has to share his/her profile details, the user's friend list, email address, timeline photos and posts with the app developers. Implicit in this condition is the catch that makes the app trace the personally identifiable data of users that helps the developers to uniquely identify, locate or contact every single user.

Similarly, the privacy policies of the MalluApps also demand that users share the personal details and friends list in order to engage with the application. Even though the app produces fun in vernacular languages such as Malayalam and Tamil, the policies of the apps are furnished in English language. By using the app, a user endorses to share basic information of the users profile, wall posts, photos and chat inbox with the app developers. Compared to Pandacat, MalluApps makes it categorical that they are accessing the personal chat box of the user too. Drawing on Nissenbaum's contextual integrity, it can be seen that both these third party applications violate the 'norms of distribution' as the user endorses to provide the profile details of his/ her friends and the data created by those people.

What becomes unethical is that although a person has the right to share his/her profile details and activities on Facebook to a third party, s/he doesn't have the right to share the list of his/her friends and their activities on Facebook to others. While endorsing the privacy policies of these apps, the user gives permission to access the details and activities of all others in his/her friends list and thus s/he eases the path of the third party to peep at others' Facebook activities. The scenario signifies a fact that the information provided by a person to his friend (to the user of the third party fun application), flows out of the context by breaching the norms of distribution.

Privacy as an Instrument of Biopolitics

The privacy policies of Pandacat reveal that the application is using Facebook's 'Remarketing pixels' that allows "the app developer and Facebook to determine the relevant target audience in order to display advertisements in reference to potential interest of the user". Remarketing pixels indirectly divulge that Facebook markets the data generated about the browsing behaviour of users to third party app developers. Fun-based third party applications have a veiled teleology of generating profit from users' data gathered from their demographic details. The two apps analysed here point to possibilities of autonomy, agency and identity of users in terms of their ability to exercise their freewill to participate in them. However, the potential of leisure that structures the consciousness or unconsciousness of users folds into regimes of biopolitics of regulation and monitoring.

Users produce labour through their participation in Pandacat and MalluApps which subsequently feeds into profit for Facebook as well as the third party application developers. These applications obfuscate users insidiously as they are completely detached from seeing, sensing or being aware that Facebook is the platform in which these applications are running from. Privacy is ceded and lost to two companies namely the applications that generate and allow users to engage with content and the Facebook platform that hosts it. In other words, third party applications emerge as subterranean entities to strengthen the potential of Facebook in dredging up data about users.

Facebook is the imperceptible active sentinel of the Panopticon. Drawing on Deleuze (1995), it can be argued that Facebook and third party applications exemplify modulations of control, open and distributed ontologies but controlled. The more layered they are, the more nuanced the control gets. Thus, the agency of users through the enticing of leisurely engagement with

content in third party applications (here) becomes mobilised in the dynamics of biopower. The 'self' slips into a certain degree of fascism that purports to control and monitor user actions and behaviour online. This reveals how the unencumbered self that is given to be believed is circumscribed by factors that work in the service of capital.

Foucault's theorisation of biopolitics explicates the politics of control of bodies through diffuse technologies; technologies mediate control and regulation. Pandacat and MalluApps operate to accumulate capital by inciting bodies to life framed by the techniques of control and measurement. The self is quantified and produced as an entity that is amenable to commodification. The self has to perform to be measured and its performances are pre-governed through the algorithms of third party applications and the hosting platform Facebook. The self in its pursuit of leisure and knowledge-production is folded into the economies of sociality and control. Users of these two applications are enmeshed in a vicious circuitry of economic capitalism and biopower, enabling the self to be quantified. The corporeal self is dematerialized to become subjects of the corporatized economy. In other words, the digital immaterial labour of users rematerializes the body into quantifiable commodities, whereas the distinction between leisure and labour diffuses and creates appraisable material bodies. Further, the materiality of bodies in experiencing leisure is overrun with the biopolitics and economic interests of the corporate. Leisure ceases to be jouissance. Leisure is the cause and result of immaterial labour performed by users in Pandacat and MalluApps. While the time spent to create data on Facebook constitute a single production for the owners of that platform, the time spent on Pandacat and MalluApps and the action which provided users' profile details and their friends' details constitute another production.

Conclusion

The analysis of the privacy policies of MalluApps and Pandacat indicate breach of privacy as mining and leaking of personal data overreach the 'context' and 'norms' of Nissenbaum's contextual integrity. The accumulation of user data by third party applications is biopolitical. These applications compile different facades and traits of data, as perceived by the algorithms already programmed to do so, and manage a stock of discrete, incoherent, modulated data where individuals are prised into dividuals. Richard Rogers (2009) calls the engineered logic of algorithms to cut individuals into smaller segmentations as post-demographics whereby the political identities are erased in favour of information politics that algorithms are ordained to carry out.

While control is exercised biopolitically by MalluApps and Pandacat to garner user data, it is being done by constructing audiences. These applications create a semblance of fun imperceptibly allowing users to indulge in the production of affective immaterial labour. Joseph Turrow and Nora Draper (2014) explain how markets and industries, ruled by algorithms, compose and make datafied audiences. Using the two applications, audiences are constructed as users devoid of agency and lulled into labour in the guise of leisure. While users get temporary leisure using these apps and feel that they are engaging in a digital platform constitutive of molecular arrangements, the privacy policies of the two applications do not correspond to their becoming-molecular through interactions with users. Rather, the policies signify a totality, not accounting for emergent characteristics, appearing as monolithic biopolitical structures. The user is reduced to a powerless entity, whose failure to understand the consequences of

not reading the terms and conditions is used as an alibi to fault him/her. On the other, it is strategically well-manicured plans that leave the user high and dry. Access commodifies the user's sense of freedom. In this context, the two applications present themselves as tools that can be engaged with for ludic purposes, while subtly projecting their regime of authority to generate data objects out of them.

The personal data acquired through the applications are used for target advertisement feeding them to the neoliberal market logic. By quantifying and commodifying the private data of the users of a particular social networking site, these fun applications manage to exercise a certain power to mould the deportment and lifeworld of users. In prevailing Indian conditions, despite the Supreme Court upholding that privacy is a fundamental right of the citizens under Article 21 of the Indian Constitution, the nuanced ramifications of such a verdict on how it will be comprehended to understand cases of data breach and online privacy are dense with ambiguities. A case is underway in the Supreme Court of India pertaining to Aadhaar and privacy. With the General Data Protection Regulation (GDPR) in European Union a progressive measure to protect data and address concerns of privacy within EU, a similar effort in India is required to curtail social media platforms from leaking, mining and selling users' data. The final verdict on Aadhaar from the apex court will explain how India's online privacy policies will course through. Until then, the privacy breach by third party applications including MalluApps and Pandacat will not come under strict scrutiny in the current digital ecosystem in India.

References

Approach paper for a legislation on privacy. (2010, November 22). Retrieved from https://cis-india.org/internet-governance/blog/privacy/c.i.s-responds-to-privacy-approach-paper

Barth, A., Datta, A., Mitchell, J., & Nissenbaum, H. (2006). Privacy and contextual integrity: framework and applications. *Proceedings of 2006 IEEE Symposium on Security and Privacy (S&P06).* doi:10.1109/sp.2006.32.

Boyd, D. (2008). Facebook's Privacy Trainwreck: Exposure, invasion, and social convergence. *Convergence: The International Journal of Research into New Media Technologies, 14*(1), 13-20. doi:10.1177/1354856507084416.

Brown, B. A. (2013). Primitive digital accumulation: Privacy, social networks, and biopolitical exploitation. *Rethinking Marxism, 25*(3), 385-403. doi:10.1080/08935696.2013.798974.

Cote, M., & Pybus, J. (2007). Learning to immaterial labour 2.0: My Space and social networks. *Ephemera, 7*(1). Retrieved from www.ephemeraweb.org

Foucault, M. (1977). Security, territory, population: Lectures at the College De France.

Fuchs, C. (2014). Digital prosumption labour on social media in the context of the capitalist regime of time. *Time & Society, 23*(1), 97-123. doi:10.1177/0961463x13502117.

G, Ananthakrishnan. (2018, March 14). Aadhaar deadline extended, Supreme Court says hold till we decide. *The Indian Express.* Retrieved from http://indianexpress.com/article/india/sc-extends-deadline-for-linking-aadhaar-to-mobile-bank-accounts-till-judgement-5096419/

Hardt, M., & Negri, A. (2006). *Multitude: War and democracy in the age of empire.* London, NY: Penguin Books.

Hull, G., Lipford, H. R., & Latulipe, C. (2010). Contextual gaps: Privacy issues on Facebook. *Ethics and Information Technology, 13*(4), 289-302. doi:10.1007/s10676-010-9224-8.

Kirkpatrick, M. (2010, January 10). Facebook's Zuckerberg says the age of privacy is over. *The New York Times.* Retrieved from https://archive.nytimes.com/www.nytimes.com/external/readwriteweb/2010/0 1/10/10readwriteweb-facebooks-zuckerberg-says-the-age-of-privac-82963.html

K S Puttaswamy vs. Union of India (August 24, 2017). Available at https://www.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf

Lipford, H. R., Hull, G., Latulipe, C., Besmer, A., & Watson, J. (2009). Visible flows: Contextual integrity and the design of privacy mechanisms on social network sites. *Proceedings of 2009 International Conference on Computational Science and Engineering.* doi:10.1109/cse.2009.241.

Nissenbaum, H. (2010). *Privacy in context technology, policy, and the integrity of social life.* Stanford, CA: Stanford University Press.

Rajagopal, K. (2017, May 3). Aadhaar data leaks not from UIDAI: Centre. *The Hindu.* Retrieved from http://www.thehindu.com/news/national/pan-aadhaar-linkage-fear-of-data-leaks-and-right-to-privacy/article18413834.ece

Rogers, R. (2009). Post-demographic machines. In A. Dekker, & A. Wolfsberger (Eds.), *Walled Garden* (pp. 29-39). Amsterdam: Virtueel Platform.

Rose, J., & Spencer, C. (2015). Immaterial labour in spaces of leisure: Producing biopolitical subjectivities through Facebook. *Leisure Studies, 35*(6), 809-826. doi:10.1080/02614367.2015.1031271.

Sriram, J. (2015, March 24). SC strikes down 'draconian' Section 66A. *The Hindu.* Retrieved from http:// www.thehindu.com/news/national/supreme-court-strikes-down-section-66-a-of-the-it-act-finds-it-unconstitutional/article10740659.ece

Swant, M. (2017, July 26). Facebook raked in $9.16 Billion in ad revenue in the second quarter of 2017. Retrieved from http://www.adweek.com/digital/facebook-raked-in-9-16-billion-in-ad-revenue-in-the-second-quarter-of-2017/

Terms and Conditions. (n.d.). Retrieved June 26, 2017, from https://malluapps.net/privacy/tl

Terranova, T. (2000). Free labor: Producing culture for the digital economy. *Social Text, 18*(2 63), 33-58. doi:10.1215/01642472-18-2_63-33.

Turow, J. & Draper, N. (2014). Industry conceptions of audience in the digital space. *Cultural Studies, 28*(4), 643-656. doi: 10.1080/09502386.2014.888929.

Wellman, B., Quan-Haase, A., Boase, J., Chen, W., Hampton, K., Díaz, I., & Miyata, K. (2006). The social affordances of the internet for networked individualism. *Journal of Computer-Mediated Communication, 8*(3), 0-0. doi:10.1111/j.1083-6101.2003.tb00216.x.