"I kind of feel resigned to the fact": A Foucauldian perspective on data privacy and social media

***** *Michael Flavin* [*1]
[1]*Kings College London*

Abstract

Social media technologies are popular and pervasive. They also entail the submission of personal data which is sold on to third parties. Users trade their personal data in return for free access to social media services. This paper uses Michel Foucault's work on panopticism, from his book of the mid-nineteen seventies, *Discipline and Punish*, to analyse users' practices on social media and their thoughts and feelings regarding the usage of their personal data. An online survey and semi-structured interviews were used to gather data. Twenty-one participants, most of whom were postgraduate students, completed a survey and four attended a follow-up, semi-structured interview. The paper argues that users adopt a fatalistic position regarding the submission of their personal data, and that users value social media services. The paper makes a significant contribution to the literature by surveying social media usage in general rather than one social media provider; by showing how users tend to curate identities on social media as a defensive strategy in relation to the fact that the data they submit does not belong to them and may be sold on; and by arguing that social media users tend not to hold social media companies responsible for the data they extricate from users.

Social media; Data privacy; Foucault, Michel; Panopticon; online surveillance.

1. Introduction

This paper uses the panopticon as a means to analyse the question of data privacy on social media. The paper defines social media as interactive online platforms enabling connection and the production, distribution and consumption of material produced in a range of modalities, including text, images and video. The paper aims to analyse users' practices with social media, to evaluate what users know about surveillance on social media and to analyse how they respond to the climate of surveillance on social media. The specific question addressed by this research is: To what extent do social media users accept loss of privacy? A similar question was posed by Krasnova et al. (2010). We are now more than a decade later and social media has risen rapidly in popularity. Now is therefore an apt time to analyse users' thoughts and feelings about data privacy. Moreover, using Foucault's work on panopticism offers particular insights on users' attitudes towards privacy infraction and how surveillance might alter behaviour. Using a sample of predominantly postgraduate students, the paper considers the extent to which users are aware that their practices on social media are recorded; that their data are being sold on to third parties; the extent to which they accept a data privacy trade-off in return for access to social media services; and the extent to which they construct authentic personae on social media.

Following a summary of Foucault's reading of the panopticon, the paper summarises its methodology and presents its findings. The paper argues that users accept, albeit reluctantly, the trade-off of their privacy in return for free access to services which are often considered necessary for their professional and social lives. Users also curate digital identities which are not always authentic but which can offset some aspects of online surveillance. In addition, users cite disparate stakeholders whom they consider responsible for data privacy, not necessarily centring on social media providers.

Michel Foucault's *Discipline and Punish* was first published in 1975. It was translated into English in 1977. The book argues that systems of judicial punishment in western societies (specifically, France) shifted from physical retribution to corrective, disciplinary treatment. Moreover, the changes coincided with the development of a capitalist economy which required plentiful, physically able and compliant labour.

One of the key concepts in the book is the panopticon, a form of prison design which enables constant scrutiny of inmates without the inmates themselves knowing if they are being observed. The very presence of the panopticon exerts an influence on behaviour. It is a low cost means of surveillance and control.

The panopticon is a useful way of thinking about surveillance in the digital age. As Cabeston (2020) notes, "Panopticon theory has witnessed a genuine revival precisely because of the growth of digital surveillance." The pre-digital panopticon, "only allows the monitoring of actions, of behaviour; it precisely does not afford insight into prisoners' minds" (Fludernik, 2017, p. 10). However, online observation can and does give insights into what people think. Users publish their thoughts and feelings on social media. That said, users curate their online personae and therefore the information published on social media is not necessarily comprehensive and authentic: Schonebeck et al. (2016) show young people are conscious of their online identities, undertaking "retrospective impression management" (p. 1482). Nevertheless, access to thoughts and feelings is a capacity of social media that was not available to the panopticon as a form of architecture for incarceration.

2. Literature Review

In *Discipline and Punish*, in the chapter titled "Panopticism," Foucault uses Jeremy Bentham's panopticon (a model of prison design proposed in the late-eighteenth century enabling constant scrutiny of inmates) to analyse how the threat of constant physical observation can be used to induce individuals to self-police their behaviour without direct oversight. Foucault's reading of the panopticon does not conflate exactly with Bentham's idea (Safaei 2020; Weinreich 2021). However, despite the distinction between Foucault's application of the panopticon and Bentham's original design, it is a valuable way of thinking about how constant online surveillance effects individual's behaviour. Manokha (2018) argues for, "the usefulness of the metaphor of Panopticon for the analyses of modern surveillance practices… not only is it still relevant but it is actually more relevant today" (pp. 230-231). The panopticon is useful for analysing how surveillance and even just the possibility of surveillance can modify behaviour. The panopticon as described in *Discipline and Punish* becomes a metaphor for a widespread system of surveillance in the digital age.

Foucault comments on the cellular structure of Bentham's panopticon: "They are like so many cages, so many small theatres, in which each actor is alone, perfectly individualized and constantly visible" (2020, p. 200). Social media, like theatre, can be a site for performance. Users can present a curated self to the world. Social media is also a state of constant, potential visibility to the network voluntarily entered into by the user; to the provider of the social media services; and to third parties to whom social media companies sell-on information.

Panopticism is well-suited to neoliberal societies encouraging individualistic perspectives and competition. Individuals connect and network on social media but they do not own the data they produce. The presence of individually targeted advertisements and political canvassing on social media evidence an individualised approach whereby advertisements are tailored to the individual's profile. Riemer and Peter (2021) state, "Facebook had, in 2007, already allowed companies and brands to create their own pages on Facebook... But from January 2012, in preparation for its Initial Public Offering…, it allowed them to advertise those pages in users' newsfeeds. Facebook now found itself under increased public scrutiny to actively search for more ways to monetise activity on its platform. This monetisation came in the form of targeted advertising." The exploitation of users' data was determined by a commercial imperative. Individuals are targeted on social media because of the commercial necessity to sell-on their data to third parties, to make, in turn, social media more attractive to investors and to make social media companies profitable.

The relationship between the watcher and the watched on social media is ultimately a relationship of power: "in the peripheric ring, one is totally seen, without ever seeing; in the central tower, one sees everything without ever being seen" (Foucault 2020, p. 202). Data contributed to social media by users are sold-on to third parties. The data create a profile which can be used by providers of goods and services and by political interests. Users make themselves available for retail and political targeting, a practice which is not the purpose of their engagement on social media but is its outcome.

Foucault states, "The Panopticon functions as a kind of laboratory of power" (2020, p. 204). The position of dominant specularity held by the social media provider enables the collection of data which support targeting for commercial and political purposes. The social media panopticon is a laboratory by allowing for experimentation, with different types of targeting being aimed at users. Retailers and political stakeholders purchase and accrue knowledge which is then put to work. Foucault also defines the panopticon as, "a figure of political technology" (2020, p. 205). It is a political technology because it enables and exemplifies the distribution of power in a neoliberal society. Users connect with each other but are under constant potential scrutiny with each unit of data they contribute. Users are a means of making profit thanks to a commercial alliance between the social media companies and other enterprises. Additional profit can be made by selling data to political interests: Manokha (2018) elaborates on the panopticon as a figure of political technology to identify, '"technologies of the self'—the manner in which panoptic settings make individuals perform on themselves, without coercion, different operations and exercises of power" (p. 220). The panopticon consolidates and condenses power, influencing practice by virtue of its presence.

Foucault further describes the panopticon as, "a design of subtle coercion for a society to come" (2020, p. 209). The coercion is subtle because, in the context of social media, a user does not see the connections that precede the appearance of an advertisement or item of political canvassing on their social media feed. Foucault published *Discipline and Punish* in

the mid-1970s: the future society it anticipated is with us two generations later. The covert organisation of power on social media is crucial to its effects: "In appearance, it is merely the solution of a technical problem; but, through it, a whole type of society emerges" (Foucault 2020, p. 216). The effects of social media are widespread. Data are accrued, packaged and sold. Targeted communications aim to shape spending patterns and political allegiances. Foucault states, "it is not that the beautiful totality of the individual is amputated, repressed, altered by our social order, it is rather that the individual is carefully fabricated in it, according to a whole technique of forces and bodies" (2020, p. 217). Identities on social media are, to a greater or lesser extent, curated, but the online persona can have greater visibility and presence than the person. The aggregated social media profile is the face the user presents to the world. The profile is also a data set for exerting commercial and political influence.

Foucault identifies three criteria evidencing what he terms a tactics of power: "firstly, to obtain the exercise of power at the lowest possible cost (economically, by the low expenditure it involves; politically, by its discretion, its low exteriorization, its relative invisibility, the little resistance it arouses); secondly, to bring the effects of this social power to their maximum intensity and to extend them as far as possible, without either failure or interval; thirdly, to link this 'economic' growth of power with the output of the apparatuses (educational, military, industrial or medical) within which it is exercised; in short, to increase both the docility and the utility of all the elements of the system" (2020, p. 218). Social media has utility, offering value to its users. It also offers use value to businesses who can segment their audiences and target their advertising. In addition, use value is available to political canvassers who can target messages based on users' individual profiles.

From a Foucauldian perspective, social media can comprise, "a power that is manifested through the brilliance of those who exercise it, a power that insidiously objectifies those on whom it is applied; to form a body of knowledge about these individuals, rather than to deploy the ostentatious signs of sovereignty" (Foucault 2020, p. 220). If social media compels individuals to regulate their behaviour it comprises a form of policing but without any evident enforcement. Data contributed to social media comprise an ever-growing body of knowledge. Moreover, it is useful knowledge to those who own the platforms because it is sold on to commercial or political stakeholders.

Foucault's analysis of the panopticon is not transferable unproblematically to the digital age. For example, Foucault states, "The arrangement of his room, opposite the central tower, imposes on him an axial visibility; but the divisions of the ring, those separated cells, imply a lateral invisibility" (p. 200). One of the most fundamental features of social media is the capacity to connect with other users. While the panopticon has monopolistic specularity, social media has diverse specularity but it also has a hierarchy of spectators, with the providers of social media services having access to all the material thereon. Moreover, the collection of data on social media and its usage thereafter is not made transparent to the individual user, even as they produce the data. Laval (2017) states, "The panopticon is… a maximizing device which, with limited means, produces very great effects. Its force is a mental, imaginary one; it lies in its power to penetrate the minds of individuals by establishing a permanent relationship between what one might do and what one would risk if one did. And this is due to the simple fact that it introduces a dissymmetry between the watcher and the watched" (p. 48). The panopticon can control practice by the fact of its presence.

Subsequent to Foucault, Krasnova et al. (2010) found a tension between the convenience and enjoyment of social media on one hand, and data privacy concerns on the other, though they argued the pros of social media usage outweighed the cons. Moreover, users self-disclosed more if they were looking for common ground with other users. In addition, Romele et al. (2017) suggest social media users voluntarily submit to a system, contributing profitable information, and Marwick and Hargittai (2019) argue social media users are largely resigned to privacy violation. Afriat et al. (2020), in a study of Facebook usage, argue, "users perceive privacy not as an integral component of one's civil rights but as a negotiable commodity traded according to societal norms" (p. 116). Privacy is itself a tradeable commodity, an abstract noun reified into an instrument in commercial exchange: privacy in exchange for access, the entrance charge for social media services. Moreover, Hafermalz (2021) argues users' fear of observation is relegated beneath users' fear of exile: users would prefer to be observed than to be excluded from the services and communities to which social media provides access. Brown (2020), in a study of Facebook users in the aftermath of the Cambridge Analytica scandal, found users accepted Facebook's practices because of the benefits offered. Usage of the service was traded for personal data. Furthermore, Afriat et al. (2020) show that user numbers for Facebook increased in the year the Cambridge Analytica scandal broke (p. 116).

This section has focused on Foucault's usage of the panopticon in *Discipline and Punish*. The next section outlines the method deployed to gather and analyse data.

3. Methods

This research analyses the extent to which social media users accept a loss of privacy, using Foucault's reading of the panopticon as a theoretical framework. The research obtained institutional, ethical approval. It comprised an online survey followed by online, semi-structured interviews (an online survey was also used by Krasnova et al. [2010] in a survey of self-disclosure practices on social media). This approach, of survey followed by interviews, was taken so that the initial findings could be elaborated upon by more in-depth questioning.

The overall methodology relates to the research question by first identifying users' social media practices and then by exploring the thought processes and choices underpinning their practices. Questions in the survey and the interviews were intended to gather data concerning participants' awareness of what can happen to information on their social media accounts; their thoughts and feelings about what happens to their data; and their continued usage of social media despite the loss of privacy. The research approach allowed for both surface level and richer data for analysis.

A convenience sample was used. The online survey was issued to a closed LinkedIn group in October 2021, comprising present and former students of a module led by the researcher. An invitation to undertake the survey was posted on the closed group. A total of 393 members were registered on the group during the time period the research was undertaken, most of whom showed little or no engagement with the group. Following the initial invitation to undertake the survey, a further two reminders were posted over a three week period. The survey was open from mid-October to mid-November 2021. A total of twenty-one responses were received. The survey questions feature as an appendix to the paper.

At the end of the survey, participants were asked if they would be willing to undertake a follow-up, online interview. A total of five students responded positively. In a follow-up query, four re-stated their willingness to participate and one declined. Four semi-structured interviews therefore took place in December 2021. The questions were written after the survey results had been read and analysed, to ensure points relevant to the research and the data gathering thus far were raised and elaborated upon. The interviews began with a warm-up question asking participants which social media platforms they used and what they used them for, an approach which was also taken by Schoenebeck et al. (2016) in a study of students' Facebook usage. The first question framed the area of enquiry and was also intended to put participants at ease. The interview questions for this paper feature as an appendix.

The results of the survey were analysed over repeated readings to identify overall patterns of social media usage, to indicate awareness of data privacy and the relationship between the two. The interview transcripts were produced contemporaneously on Microsoft Teams and were saved. Initial codes were drawn from the interviews using the panopticon as a theoretical framework, including fatalism regarding surveillance, the curation of digital identities, and reflections on responsibility for data privacy.

Content analysis (Bryman 2016) was used to analyse the interviews. The analysis was interested in both manifest and latent content: Bryman (2016) argues content analysis is as interested in omissions as in what does get reported (p.287; see also, Krippendorff [2013, p.360]). The content analysis in this paper has a directed approach (Hsieh & Shannon 2005); Foucault's chapter on Panopticism in *Discipline and Punish* was used to frame the analysis of participants' practices on social media.

Overall, the research methodology enabled a detailed account of the participants' usage of social media, awareness of data privacy and the relationship between the two in practice. The qualitative data from the interviews illustrated the findings from the survey. The interviews allowed for the exploration of the processes that lay behind the practices revealed by the survey findings (Bryman 2016, p. 645). The analysis fed forward to the conclusion which returned to the research question.

Having discussed the research method, the next section summarises the results of both the survey and interviews.

4. Results

The sample of twenty-one comprised predominantly postgraduate students (n.15). There were also three undergraduate students, one postgraduate researcher, one in employment, and one participant neither in employment nor studying. A significant majority were in the age group 18-30 (n.16); the other five were 31-49. The sample featured eleven different nationalities, the most numerous being Indian (n.7), though the analysis did not segment the data by nationality, as not all participants were resident in their home country. Moreover, two respondents did not state their nationality. The most commonly used social media apps in the survey were Instagram and YouTube (n.17); Whatsapp (n.16); LinkedIn (n.15); and Facebook (n.14).

Sixteen respondents stated they were worried about what happens to the data they enter on social media, and six replied "not at all" in response to the question, "To what extent do you trust social media platforms?" (the other responses were "partly" [n.7] and "slightly" [n.8]). Eighteen respondents stated they were more cautious about what they said online than they were in everyday communication. Eleven had deleted at least one social media app over privacy concerns; twelve had made purchases that had been advertised to them on social media. Nine of the respondents stated that their support for a political cause had been sought on social media.

Eleven of the sample were currently in some form of employment, of whom eight used social media in their job. Twenty of the sample were currently studying, of whom sixteen used social media to support their learning. Nineteen used social media to support their social lives.

In response to the question, "How important is social media to you?", two (10%) said "very important"; thirteen (62%) said "quite important"; three said "neither important nor unimportant" (14%); two said "not very important" (10%) and one said, "not important at all" 5% (figures rounded to whole percentages). The responses were weighted towards social media apps being at least quite important in respondents' lives, as shown in figure 1. Over 70% of the sample said social media was either "very important" or "quite important" to them (71.4%, to one decimal place).

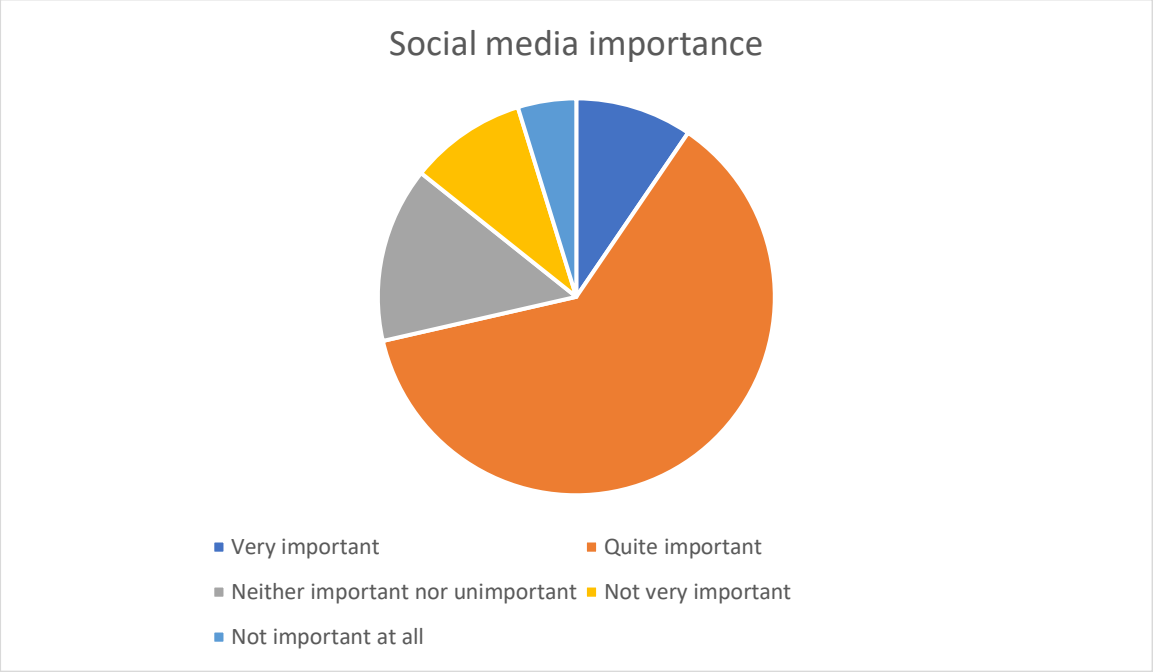

Figure 1. Respondents' evaluation of the importance of social media to them.

In response to the question, "Are you content to contribute your personal data in exchange for social media services," seven respondents stated "yes" and thirteen stated "no" (one did not respond). Sixteen of the full sample of twenty-one were aware that data they contributed on social media did not belong to them. Eighteen were also aware that social media companies can sell-on their personal data to providers of goods and services, and to political interests.

Following the survey, four semi-structured interviews were undertaken in December 2021. For the purposes of this paper, the participants are labelled A, B, C and D.

One of the most notable traits in the interviews was fatalism. Participant A stated: "it's kind of this inevitable decline of privacy… I don't like it because I can find myself in some ways self-censoring. Of course I don't like people knowing what I am searching or doing because I do appreciate privacy. But likewise, I kind of feel resigned to the fact." Participant B stated, "I feel like I'm never free from that kind of um, like, monitoring... because it's inevitable for me as someone living in the city to live with a laptop or mobile phones, internet, social media and so forth in order for me to connect with others and do my work… uhm, monitoring, like, me on the digital space is something that I am, I don't like… So yeah, overall I'm very uncomfortable, like my hope will be they will not track me down, like, my activities online, but that's not the reality, they always do." Participant C stated, "the way they are tracking your phone, your whatever you do, your location, everything, that's very very scary for me." Participant D stated, "my information, what I like, what I don't like, I wouldn't want it to be known and kept in a database, but that's what you know social media does. And so I try to keep it a bit, uh, concealed as much as I can, but I'm not very good at doing it. I try not to think about it too much because it leads me to paranoia. Like I, I'm aware of it, I know that it's there and I know that… But I think that's just how the world has become like, just this is the new way of communication. This is what's happening in the world right now, and I don't know how much control we can have over it."

The participants also spoke of the curation of digital identities. With regard to their own digital identity, Participant A stated, "You're not painting a fake picture of your life because these things have actually happened, but you're only showing the big positives and you're sort of implicitly avoiding all of the negative aspects, so you're sort of painting the best possible picture of your life." Participant D stated, "I only post when there's something remarkable that I want to share, like I make a conscious decision to share something with my friends."

The participants were judgmental of how others curate their digital identities. Participant A stated, "In most cases it's not fake, but, uh, I think again, it's a very idealized image, what they want to share with the world." Participant B stated, "they tend to share moments that are extraordinary, happy or interesting in their lives." Participant C stated, "putting in some pictures or some personal content to get validation from an outside world. That is not something that drives me" and, "I know of a few friends who wake up at night just to check how many views their recent status or recent stories... I mean, you know when we go out for dinner, they are busy clicking the pictures of the dishes instead of enjoying it with the company." Participant D stated, "I see, you know, the profiles. I understand that some people use Instagram as a business and they, you know, project a certain persona so that they get more likes and more followers and more, you know, like profit out of it."

Participants were clearly aware of the value of social media. Participant B stated, "like even a decade ago, we had to pay a lot of money to make international calls or had to put a lot of effort and energy in order to find my friend or friends who lost contact years ago and I think social media allowed me and many other people to restore that kind of relationship naturally," and participant D stated, "I use it [Instagram] to find different destinations, like I use the hashtags a lot just to see what people are doing in like different parts of the world and always when I have like a holiday coming up, I would browse photos and see, you know, what are the places that are worth traveling to. I feel Instagram gives a more recent account of

that." Participant C stated, "We can survive, you know we can live without social media, but I feel that it makes things much easier, especially for example, in my case, a lot of my friends are abroad or almost 80% of them are abroad and so I feel it's really, uh, interesting, like it's a really useful tool to keep connected to those, uh, in your network… and even connect with other people you know across the world… so it's a tool that we can use to our benefit, but it also has, you know, many things we should be aware of."

In the interviews, participants gave different answers when it came to the question of who was responsible for data privacy on social media. Participant A stated, "I think it is the responsibility of the company, but I think it's the responsibility of the state to legislate to make sure the company is protecting the privacy and also I suppose it's the responsibility of the state to punish in cases in which there is misuse of my data." Participant C stated, "I think when it comes to data, no one can work in isolation. Companies cannot take full responsibility because they want money and then government wants the data of its citizens as well. So partly it's dependent on them. I mean, in the sense they should be more open and more vocal about what they're collecting... But they are not." Conversely, participant D stated, "I feel that I am responsible for any content that I put online, so I need to be managing that with, you know, consciousness, with greater awareness that, you know, as to how it's going to be available and for how long it's going to be available as well. But I feel that for example Facebook, I stopped using it. I used to post a lot on Facebook and then I stopped using it because I found out that some default settings, they just change by themselves. Like sometimes there's an update on the app and then you have to manually go in and check." Participant D added, "social media tries to kind of get as much information and as much data from you as possible as they can get their hands on. But you have to be aware of how you manage that."

5. Discussion & Conclusion

This paper analyses the extent to which social media users accept their loss of privacy. The paper argues the practice of surveillance is quotidian and accepted, albeit reluctantly, as a *de facto* cost for access to social media services supporting professional and personal practice. The participants in this research largely exempted social media companies from responsibility for data privacy. Foucault identifies, "a machinery that is both immense and minute, which supports, reinforces, multiplies the asymmetry of power and undermines the limits that are traced around the law" (2020, p. 223). Power is asymmetrical on social media because users do not own the data they contribute and cannot determine how their data are sold on, or to whom, or for what purpose. Each contribution to social media is a potential addition to an immense body of information which can be used for purposes over which users have no control. Control, instead, rests in, 'a handful of transnational, profit-seeking panoptic networks' (Kwet 2020, p.1).

The usage of social media can be politically progressive: it played a role in the Arab Spring (Lance-Bennett & Segerberg 2012) and in the campaign against the violent excesses of the Special Anti-Robbery Squad in Nigeria (Akinyetun 2021). However, Wolfsfeld et al. (2013), in a study of the Arab Spring, argue social media followed protest rather than catalysing it. Social media also played a role in the growth of the Black Lives Matter movement (Hockin-Boyers & Clifford-Astbury 2021) following the murder of George Floyd in 2020, enabling support for the movement to be scaled up (Mundt et al. 2018). The participants in this study are aware of the drawbacks of using social media but continue to use it anyway, making cost-

benefit calculations and using social media services extensively, albeit with discomfort and apprehension.

The curation of distinct digital identities is one way of managing the tension between data privacy and access to social media. Participants in this research sculpted their own identities and were aware of others undertaking similar curatorial practices. The surface appearance they presented to the social media interface was a conscious act of construction. Furthermore, participants could and in some cases had deleted apps over privacy concerns, itself an act of digital identity curation. Participants were resigned but not inactive, creating digital personae rather than broadcasting unadorned experience. However, online surveillance has access to layers beneath the surface, such as searches undertaken by the user, and thus the face presented to the social media service is only a veneer for the corpus contributed to the providers of social media services and the third parties to whom they sell on data. Identities on social media are constructed and curated but they produce a substantial residue which is still visible to the providers.

The interview participants were divided over who was responsible for looking after their data: responses mentioned the government, the social media companies and the individual user, suggesting neoliberal principles are not ubiquitous but neoliberal practices, of individual actions unsupported by governmental protections, are recognised as a fact of existence. Personal data are sold on and individuals are commodified. Interview responses suggested the social media companies have some responsibility for privacy but not full responsibility, nor were the social media companies held to be primarily, predominantly responsible for users' data privacy. Users in this study, in common with Afriat et al. (2020), stated individuals are responsible for data privacy, yet the present study also shows users attributing responsibility to governments and, to a lesser extent, social media providers. The fact that social media providers are partly or largely absolved from responsibility implies a level of acceptance of their data gathering practices as a feature of their composition and as an exemplification of their ongoing activity. Users know they are being watched but tend not to hold the watchers responsible. Users' exculpation of social media companies may reflect effective corporate communication on the part of the companies, but it may also reflect a perspective on the part of users which is neoliberal in the sense that the individual has to take responsibility for their actions in a largely unprotected online space, despite not having produced the social media services or their data gathering practices.

The use of a college-educated, predominantly postgraduate sample in this paper is not representative of wider populations: Schonebeck et al. (2016) argue, "A college-going population may have been better educated about appropriate online behaviour" (p. 1484). The sample, however, is useful for considering how users in higher education interact with social media and questions of data privacy. Social media can be and is used to support learning. Furthermore, using proprietary, university technology enhanced learning systems requires the submission of personal data. Higher education providers might usefully reflect on the ethical aspects of social media usage for education, given that the data are scrutinised, packaged and sold on. Individual educators have to manage a balance between privacy and openness (Cronin 2017).

This paper works from a small sample; a larger sample would be necessary to enhance the reliability and validity of the research findings. That said, this paper does show that the research participants were aware of how their data were used yet continued to use the services. In practice, the price of exclusion was perceived as greater than the value of their

personal data. Most of the survey respondents (n.13) were not content to contribute personal data yet the interview transcripts indicated that they did make the trade based on an evaluation of the costs versus the benefits. Foucault (2020) argues "Visibility is a trap" (p. 200). The findings of this research suggest visibility is a trade-off more than a trap, but a trade-off made from a negotiating position of weakness because the cost of exclusion is perceived as greater than the cost of intrusion.

Social media companies are established and mature businesses. They are highly popular and pervasive. Their profitable practices of selling-on personal data are also entrenched. Political struggles, as evident on social media, have more of a wildfire quality, though they also hold the potential for co-ordination and transnational, even global alliances. However, at present, this study argues that social media services are more commonly sites for the expropriation of data which are sold-on for profit, rather than for politically progressive networking, though social media retains progressive potential. Participants in this study traded their personal data for access to services, yet their disposition in so doing was often reluctant and apprehensive. As participant C stated: "even though… all my privacy settings were, uh, you know, set to very very private mode, it was still tracking all the information. It was still seeing all those things." Judging from participants' practices, exclusion from social media services was a price they were unwilling to pay because of the extent to which they relied on social media to support their personal, educational and professional lives. Users can feel objectified but accept, on a practical level, their objectification. Foucault (2020) argues, "The ideal point of penalty today would be an indefinite discipline: an interrogation without end, an investigation that would be extended without limit to a meticulous and ever more analytical observation, a judgement that would at the same time be the constitution of a file that was never closed" (p. 227). In the era of the Pandemic, the scope and penetration of personal data and online surveillance intensified (Couch et al. 2020). Social media is regarded as a necessary asset, not a nuisance or penalty, but it has the potential to penalise because it comprises a file that is never closed, gathering information ceaselessly.

References

Afriat, H., Dvir-Gvirsman, S., Tsuriel, K., & Ivan, L. (2020). "This is capitalism. It is not illegal": Users' attitudes toward institutional privacy following the Cambridge Analytica scandal. *The Information Society*, *37*(2), 115-127, https://doi.org/10.1080/01972243.2020.1870596

Akinyetun, T. S. (2021). Reign of terror: A review of police brutality on Nigerian youth by the Special Anti-Robbery Squad (SARS). *African Security Review*, *30*(3), 368-385, https://doi.org/10.1080/10246029.2021.1947863

Brown, A. J. (2020). "Should I Stay or Should I Leave?": Exploring (Dis) continued Facebook Use After the Cambridge Analytica Scandal. *Social Media+ Society*, *6*(1), doi: 10.1177/2056305120913884

Bryman, A. (2016) *Social Research Methods*, 5th edn, Oxford: Oxford University Press.
Cabestan, J. P. (2020). The State and Digital Society in China: Big Brother Xi is Watching You!. *Issues & Studies*, *56*(1) doi: 10.1142?S1013251129400032

Couch, D. L., Robinson, P., & Komesaroff, P. A. (2020). COVID-19—extending surveillance and the panopticon. *Journal of Bioethical Inquiry*, *17*(4), 809-814, https://doi.org/10.1007/s11673-020-10036-5

Cronin, C. (2017). Openness and Praxis: Exploring the use of open educational practices in higher education. *International Review of Research in Open and Distributed Learning*, *18*(5), 15-34, https://doi.org/10.19173/irrodl.v18i5.3096

Fludernik, M. (2017). Panopticisms: from fantasy to metaphor to reality. *Textual Practice*, *31*(1), 1-26, https://doi.org/10.1080/0950236X.2016.1256675

Foucault, M. (2020 [1977]). *Discipline and Punish: The birth of the prison*, London: Penguin.

Hafermalz, E. (2021). Out of the Panopticon and into Exile: Visibility and control in distributed new culture organizations. *Organization Studies*, *42*(5), 697-717, https://doi.org/10.1177/0170840620909962

Hockin-Boyers, H., & Clifford-Astbury, C. (2021). The politics of #diversifyyourfeed in the context of Black Lives Matter. *Feminist Media Studies*, https://doi.org/10.1080/14680777.2021.1925727

Hsieh, H.-F. & Shannon, S.E. (2005). Three approaches to Qualitative Content Analysis. *Qualitative Health Research*, *15*(9), 1272-1288, https://doi.org/10.1177/1049732305276687
Krasnova, H., Spiekermann, S., Koroleva, K. & Hildebrand, T. (2010). Online social networks: why we disclose, *Journal of Information Technology*, 25, 109-125, https://doi.org/10.1057/jit.2010.6

Krippendorff, K. (2013) *Content Analysis: An introduction to its Methodology*. 3rd edn, London: Sage.

Kwet, M. (2020). Fixing Social Media: Toward a democratic digital commons. *Markets, Globalization and Development Review*, *5*(1), 1-20, https://doi.org/10.23860/MGDR-2020-05-01-04

Lance-Bennett, W. & Segerberg, A. (2012). The logic of connective action: Digital media and the personalization of contentious politics. *Information, Communication & Society 15*(5): 739-768, https://doi.org/10.1080/1369118X.2012.670661

Laval, C. (2017). 'The invisible chain': Jeremy Bentham and neo-liberalism. *History of European Ideas*, *43*(1), 34-52, https://doi.org/10.1080/01916599.2016.1251718

Manokha, I. (2018). Surveillance, panopticism, and self-discipline in the digital age. *Surveillance & Society*, *16*(2), 219-237, https://doi.org/10.24908/ss.v16i2.8346

Marwick, A., & Hargittai, E. (2019). Nothing to hide, nothing to lose? Incentives and disincentives to sharing information with institutions online. *Information, Communication & Society*, *22*(12), 1697-1713, https://doi.org/10.1080/1369118X.2018.1450432

Mundt, M., Ross, K., & Burnett, C. M. (2018). Scaling social movements through social media: The case of Black Lives Matter. *Social Media+ Society*, *4*(4), doi: 10.1177/2056305118807911

Riemer, K., & Peter, S. (2021). Algorithmic Audiencing: Why we need to rethink free speech on social media. *Journal of Information Technology*, *36*(4), https://doi.org/10.1177/02683962211013358

Romele, A., Gallino, F., Emmenegger, C., & Gorgone, D. (2017). Panopticism is not enough: Social media as technologies of voluntary servitude. *Surveillance & Society*, *15*(2), 204-221, https://doi.org/10.24908/ss.v15i2.6021

Safaei, S. (2020). Foucault's Bentham: Fact or Fiction? *International Journal of Politics, Culture, and Society,* https://doi.org/10.1007/s10767-019-09342-7

Schoenebeck, S., Ellison, N. B., Blackwell, L., Bayer, J. B., & Falk, E. B. (2016). Playful backstalking and serious impression management: How young adults reflect on their past identities on Facebook. In *Proceedings of the 19th ACM conference on computer-supported cooperative work & social computing*, 1475-1487.

Weinreich, S. J. (2021). Panopticon, Inc.: Jeremy Bentham, contract management, and (neo) liberal penality. *Punishment & Society*, https://doi.org/10.1177/14624745211023457

Wolfsfeld, G., Segev, E., & Sheafer, T. (2013). Social media and the Arab Spring: Politics comes first. *The International Journal of Press/Politics*, *18*(2), 115-137, https://doi.org/10.1177/1940161212471716

Appendix 1 - Social Media Survey

1. What is your age

18-30 / 31-49 / 50+
Prefer not to say

2. What is your nationality

Nationality (text box)
Prefer not to say

3. Are you
   An undergraduate student
   A postgraduate student
   A postgraduate researcher
   In employment
   Not in employment nor studying
   Prefer not to say

4. What social media platforms do you use?
   Facebook
   Instagram
   Twitter
   LinkedIn
   YouTube
   WhatsApp
   Weixin / WeChat
   Tik Tok
   Snapchat
   Other
   None of the above

5. Do you worry about what happens to the data you enter on social media?

Yes/No

6. To what extent do you trust social media account platforms?
   Fully/Partly/Slightly/Not at all/Don't know or no opinion

7. Are you more cautious about what you say online than you are about everyday communication in person?

Yes/No

8. Have you ever deleted a social media app over privacy concerns?

Yes/No

9. Have you ever purchased anything that was advertised to you on social media?

Yes/No

10. Has your support for a political cause ever been sought on social media?

Yes/No

11. If you are in employment, do you use social media in your job?
    Yes/No/Not currently in employment

12. Are you studying? If so, do you use social media to support your learning?
    Yes/No/Not currently studying

13. Do you use social media to support your social life?
    Yes/No

14. How important is social media to you?
    Very important/Quite important/Neither important nor unimportant/Not very important/Not important at all

15. Are you content to contribute your personal data in exchange for social media services?
    Yes/No

16. Are you aware that data you enter on social media does not belong to you?
    Yes/No

17. Are you aware that social media platforms can sell-on your details to providers of goods and services, and to political interests?
    Yes/No

We may conduct follow-up interviews, which will be conducted online. Are you willing to participate in a follow-up interview? If so, please provide an email address.

Do you have any further comments?

Thank you for completing this form.

Appendix 2 – semi-structured interview questions

Can you start by summarising what social media apps you use and what you use them for?
Are there any social media apps you used to use but have stopped using, or use a lot less? Why is that?
Have you ever deleted a social media app? If so, why?
How do you feel about the fact that your data on social media can be sold on?
To what extent do you accept the trade off between access to social media services and the selling-on of your personal data?
Thinking about the personae you maintain on social media apps, to what extent are they authentic?
How authentic are other people's social media personae?
Do you need social media? Do you think you could easily do without social media?
Who do you think is responsible for managing your data privacy?
Overall, how do you feel about being the subject of digital surveillance?