Resisting Commodification: Subverting the Power of the Global Tech Companies

Maria Bäcke

Senior Lecturer of English, Guest Researcher and Co-Leader CCD,
Department of Language, Aesthetic Learning, and Literature, School of
Education and Communication, Jönköping University, Jönköping, Sweden
maria.backe@ju.se

Abstract

In our digitised world, information and communication technologies (ICTs) are used everywhere. In schools all over the world the well-known, easy-to-use, and highly affordable Google Education is used, but is this a safe and sustainable solution? A number of services online are free in terms of users not having to pay any money for their usage, but many companies, of which Google is one, instead make their money from the exploitation of what is labelled non-personal user data, Big Data, which is harvested from the users of their free services. This type of data mining or data harvesting can be used for other purposes as well, such as for intelligence reasons, where a foreign power may capitalise on user data from another country, but it may also be to control a country's own population. Asymmetrical power distribution is inevitable and, drawing on Deleuze and Guattari's theories of power and subversion, my aim is to increase the awareness of the non-monetary costs involved in the choice of ICTs and highlight ways to shift the inherent hierarchic power. A text analysis, based on policy documents and articles focusing on online privacy, data harvesting and user commodification, studies how legislators, journalists, as well as governmental and other organisations negotiate and sometimes subvert the hierarchic power of the global tech companies in order to protect privacy, integrity and democracy as well as the profit margin of companies. The paper highlights the need for legislation and education, an enhanced ICT literacy, in the field.

Keywords

data mining – data harvesting – Big Data – Google – Facebook – ICTs – commodification

Introduction

We live in an increasingly digitised world and the events during the Covid-19 pandemic, highly relevant at the time of writing, have underlined this further for many people as more and more of us are working from home and/or receive distance education to an even larger extent than previously. With this as a backdrop, are we certain that the digital tools we are using every day are safe? Are we aware of the hidden costs of “free” technologies? Many people use Google’s services, and schools are no exception. Since Google Education provides a highly affordable solution, many schools all over the world turn to this very well-known, and easy-to-use platform, often with the Google Chromebook included in the package. However, is Google’s service, G Suite for Education, a safe and sustainable solution for the world’s children?

We may share non-personal information publicly and with our partners – like publishers or connected sites. For example, we may share information publicly to show trends about the general use of our services.
(GOOGLE G SUITE)

As this quote implies, the user data, albeit non-personal data (the definition of personal and non-personal will be discussed below) or “Big Data,” generated by under-aged children can be used by Google in accordance with the privacy notice (Lindh & Nolin 2016). Children’s data are being harvested, just as the data of anyone using Google’s search engine, e-mail services or Google docs is, but the harvesting of children’s data might seem more malicious since they are minors and have no possibility of opting out. They are forced to pay for their school’s use with their data. Generally, little is being heard about the downsides and potential hazards of data harvesting/data mining (both concepts are used interchangeably and refer to the analysis of non-personal data extracted from various online services) or user commodification (revenue based on the selling of data generated by users, discussed further below). The same attitude seems to be prevalent in many other countries all over the world and extends to social media platforms, such as Facebook, and services like TikTok. An asymmetrical distribution of power is inherent in this situation. In this paper, drawing on Gilles Deleuze and Felix Guattari’s (1986) theories of power and subversion, my aim is to highlight how everyday technical solutions, such as Google’s services and those of Facebook and companies with similar business models, involve non-monetary costs for individual users. I also aim to highlight the potential for subverting the global tech companies’ commodification of users. By performing a text analysis on policy documents and articles on online

privacy, data harvesting and user commodification, I will study how legislators, researchers, journalists, as well as governmental and other organisations argue and work to subvert the hierarchic power of the global tech companies in order to safeguard privacy, integrity and democracy.

Theoretical Framework

The internet is a neutral infrastructure of cables and routers. In itself, the internet does not regulate any type of usage. It is a *smooth space*, to use Gilles Deleuze's and Félix Guattari's concept, but it is also a space that can be regulated, *striate*, and used for control and surveillance, as is the case for some companies and in some more authoritarian countries in the world. Smooth space, according to Deleuze and Guattari, is open, anti-authoritarian, flexible, but also, as perceived by some people, uncontrolled, uncontrollable and, therefore, unsafe. Striate space, in turn, is controlled, hierarchic, regulated, but can also become too rigid and too oppressive, according to others. Between these poles there is constant negotiation and most social contexts and nation-states with reasonably balanced societies usually hover somewhere in the middle on this scale; there is a balance between (state) regulations and the freedom of the participants/citizens. What "freedom" actually means is different from individual to individual, but here it indicates the liberty to choose and invokes the concept of free will. The general rule is that striation aims to bring the smooth under its control, while the smooth uses its tools to subvert the same control (Deleuze & Guattari 1986). Moreover, the smooth contains the seed of the striate, as societies or contexts that are too unregulated tend to yearn for the safety of regulation and stability, whereas people in a too regulated and/or too hierarchic context tend to yearn for more agency (an individual's ability to act and decide for themselves in certain social contexts), freedom and flexibility. From Deleuze and Guattari's perspective – on an international, a national, a local, as well as an individual level – power is constantly being negotiated in the social space as freedom, flexibility, and agency is set in opposition to control, surveillance, and status quo.

Depending on the aims and values of a country/company/organisation, leadership is either trying to allow citizens/employees/participants a smooth space to create whatever they wish to create within the limits of the law, or restrict it's the same, perhaps by superimposing striations using surveillance or other types of control to underscore and maintain hierarchic power. Values within a certain social or cultural context are usually either repressive or supportive. This line of thinking can be applied on a digital context such as the

internet as well. It used to be viewed as an infinite smooth space, where anyone surfing its metaphorical waves was free to discover, do or create anything s/he wanted. The striations were its communication protocols, but these consisted of what was perceived as neutral code with no power to regulate or limit the internet users' thoughts or ideas. Paradoxically, digital tools have proven useful for authoritarian leadership in order to implement panoptical, striate control measures. In liberal or democratic countries, a somewhat smoother, democratic, liberal and open public sphere has been created, although still regulated by free speech laws, libel laws and human rights conventions. As authoritarian and liberal thought-structures clash, both sides fight for their interpretation of, and perspective on, digital space.

Method

This paper has used textual, already published, sources throughout. To perform a textual analysis means reading "closely," critically and independently, to read "with special attention" (DuBois 2) and look for recurring indications of various types of tensions, such as ambiguity, irony or paradoxes, patterns, underlying ideologies, preconceived ideas, omissions or contradictions. Jan Van Looy and Jan Baetens (2003) argue that "there is a sense of hostility between the reader and the text. The text is never trusted at face value, but is torn to pieces and reconstituted by a reader who is always at the same time a demolisher and a constructor" (10). This may seem overly violent, but there is some truth in the description of how a textual analyst approaches a text.

For the purpose of this analysis, my main focus was to find examples of how people think about and chart, negotiate and subvert the power of the globalised information technology corporations. Sources such as the legal frameworks regarding online privacy within the EU, India, Brazil, the U.S., and Nigeria – countries and regions representing various parts of the world but by no means intended to be exhaustive or selected to provide a full picture of the situation in the world – provide the backdrop for the analysis. Articles communicating and commenting on these regulative frameworks (in total 13 texts) add to this backdrop. Using keywords such as "Google" + "user data," "Google Education" + "user data," "Facebook" + user data," "data mining," "data harvesting," and "user commodification" and their equivalents in Swedish, Danish, and German, I searched for academic articles (17) and monographs (8) in the academic databases. In 2019, as I began the research for this paper, only 14 were related to the topic. Today (April 2021), the number has increased significantly, and three new-found articles from 2020 and 2021 have been included. Using the same

search keywords in the same languages, illustrating aspects of power inherent in digital applications, online tools, data harvesting, and the commodification of user data, online search engines (DuckDuckGo, Bing and Google) were used to find newspaper articles, company information/texts, as well as texts written by some non-profit/non-governmental organisations. Again, these were few in late 2019, but the number has increased (April 2021). The hits include texts from newspapers (17), companies (5) and non-government organisations (4). Since the topic is new, most texts are recent. The criteria for inclusion/exclusion are linked to the abovementioned keywords, but another limitation is that this paper was initially written for a conference in Mumbai, India. Therefore, the lion's share of the material is geared towards India (in a Global South context) and the EU (in a Global North context).

A Brief Outline of this Paper

In order to show how global tech companies have succeeded in creating platforms from which they wield more power than elected governments, and exemplify how legislation, education, journalists and organisations have worked together to resist and subvert commodification, this paper begins with "Legislation and regulation," providing a brief outline of data protection regulations in selected countries and regions around the world. The next section, "The need to build ICT literacy and the impact of Google Education," explores how the adoption of Google Education in schools around the globe has led to growing critique of the company's business model, which involves non-disclosed data harvesting. The next section, "Personal versus non-personal data and the commodification of users," discusses user commodification in the Global North as well as in the Global South and draws attention to Google's, but also Facebook's, strategies for exploiting user data and enrolling new users. "The dichotomised relationship between the digital Global South and Global North" highlights arguments against user commodification used successfully in the Global South and the fight against negative effects of digital colonialism on democracy and human rights. "Online security and issues of trust" broadens the focus and addresses the impact of similar technical solutions implemented by companies, but sometimes also by countries, in their efforts to gain access to user data not only for profit but for the authoritarian control of citizens. The ethical standards of companies and countries are in focus. The penultimate section, "What can be done?" highlights how subversive tactics, underpinned by widely disseminated societal and technical know-how, might be used to subvert striations set up by the global tech companies. The conclusion draws

on the differences between value systems to underline how legislation and education, an enhanced ICT literacy, can become, and in some cases already are, tools to protect privacy, integrity and democracy against the owners of non-personal data.

Legislation and Regulation

The vast majority of people wants to feel secure in digital contexts. Hence, laws and regulations are created as striations intended to safeguard private citizens, to level the playing fields vis-à-vis global tech companies and facilitate individual autonomy, smooth space, online. In the following example from the European Union, private citizens are secured against the misuse of *personal data*. One result is that the smooth space of the internet becomes slightly more striate for global tech companies like Google and Facebook and slightly smoother for the individual users. As indicated below, the “rights and freedoms of natural persons” are in focus. Article 1 in the European Union General Data Protection Regulation [GDPR] outlines the subject-matter and the objectives, which came into effect in 2016:

1. This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.
2. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.
3. The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data. (Intersoft Consulting)

Of particular interest here is the phrase “personal data” in the GDPR as opposed to the above-mentioned non-personal data in Google’s privacy notice. GDPR Article 4 provides the following definition for “personal data” (GDPR.EU):

‘Personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

This means that information/data that is not directly traceable to a “natural person,” i.e. not “legal persons” (often companies or organisations) or people who are no longer alive (GDPR.EU), is labelled non-personal data can be gathered without any problems. It is worth noting that the

GDPR also has extra-territorial effect. An organization that it is not established within the EU will still be subject to the GDPR if it processes personal data of data subjects who are in the Union where the processing activities are related “to the offering of goods or services” (Article 3(2)(a)) (no payment is required) to such data subjects in the EU or “the monitoring of their behaviour” (Article 3(2)(b)) as far as their behaviour takes place within the EU. (DLA PIPER)

There is, somewhat incongruously, no definition for “non-personal data” in the EU regulations. It seems to be implied that non-personal data simply is the antonym of personal data, i.e. anonymised material or data where all personal information is absent, and as such free to use and move out of the EU. Drawing on information from sources such as the *Electronic Frontier Foundation*, *The Guardian*, and *The Atlantic*, non-personal data may include anonymized surf, scanned e-mails, medical records, search and consumption statistics and habits, the usage of apps, information about physical location and much more (Cyphers 2020; Curran 2018; Fussell 2019). Although anonymised, the data gathered may thus provide information about for instance the attitudes and consumption patterns of an entire age group or people in a certain region. Non-personal data is often synonymous to “Big Data,” although the former is slightly more descriptive, and will therefore be used throughout this paper.

As indicated, the EU regulations have introduced a certain amount of striation for the large internet corporations and drawing on legislative examples from a few other large countries in the world, it is evident that Brazil in 2018 implemented a legislation that in many parts resembles the EU’s GDPR (DLA Piper). In the material related to the United States, however, DLA Piper highlights the fragmented nature of its data protection laws, as many of the states have their own laws. There are federal laws (i.e. the Family Educational Rights and Privacy Act, FERPA, from 1974 and the Children’s Online Privacy Protection Act, COPPA, from 1998 (Krutka, Smits & Willhelm 2021)) protecting some aspects of student’s personal data. No new federal legislation regulating the use of private data seems to be on the horizon in the U.S.

In India, already regulated by the Information Technology Act from 2000 and the Information Technology (Reasonable Security Practices and Procedures

and Sensitive Personal Data or Information) Rules (Privacy Rules) adopted in 2011, the new Personal Data Protection Bill, which is under way, is intended to

protect the autonomy of individuals in relation to their personal data, to specify where the flow and usage of personal data is appropriate, to create a relationship of trust between persons and entities processing their personal data, to specify the rights of individuals whose personal data are processed, to create a framework for implementing organizational and technical measures in processing personal data, to lay down norms for cross-border transfers of personal data, to ensure the accountability of entities processing personal data, to provide remedies for unauthorized and harmful processing, and to establish a Data Protection Authority for overseeing processing activities. (DLA PIPER, INDIA)

The focus of this Indian law is thus, again, personal data and the measures to secure the same.

In Nigeria, a similar pattern can be discerned. A number of laws regulate the use of personal data, and the Freedom of Information Act from 2011 is intended to “protect personal privacy. Section 14 of the FOI Act provides that a public institution is obliged to deny an application for information that contains personal information unless the individual involved consents to the disclosure, or where such information is publicly available” (DLA Piper, Nigeria). With this very brief outline of internet privacy laws, the tentative conclusion is that many countries/regions have implemented some degree of striation to protect users of digital services from exploitation.

Moving back to an EU setting, it is clear that the GDPR has a dual objective, as it “already provides for the free movement of personal data within the Union, next to its primary goal of protecting personal data” (European Commission 2020a). The “Regulation on the free flow of non-personal data” (2019, European Commission 2020b) stresses that

Data is an essential resource for economic growth, competitiveness, innovation, job creation and societal progress in general.

Data driven applications will benefit citizens and businesses in many ways. They can:

- improve health care
- create safer and cleaner transport systems
- generate new products and services

- reduce the costs of public services
- improve the sustainability and energy efficiency (EUROPEAN COMMISSION 2020b)

As a result, the GDPR and the “Regulation on the free flow of non-personal data” regulations enable as well as encourage the free movement of *personal as well as non-personal data* within the EU, whereas only non-personal data can be transferred outside of the EU. Based on the above quote, the free movement of data is allowed for the greater good. Questions like “from whose perspective and based on what criteria are these beneficial?” and “are there sanctions for companies or organisations that use the data in ways that would be harmful (again, based on what criteria)?” arise. Neither data harvesting nor user commodification are mentioned as potential hazards and it seems as if this regulation instead eases striation for the companies, particularly those within the EU, highlighting a certain protectionism vis-à-vis companies from outside the EU.

The main similarity between the legislations in the countries mentioned above is the aim to safeguard citizens’ personal data. As none of them explicitly protects non-personal data, this type of legislation offers some striation as safety measures for citizens, while simultaneously providing a measure of smooth space for the companies, especially for those within the EU. Examples of how India is interpreting its legislation to protect Indian users can be found below.

The Need to Build ICT Literacy and the Impact of Google Education

The EU is not alone in viewing the internet, and the services enabled by it, as essential tools with huge potentials for economic growth. ICT literacy is a priority all over the world. Digitisation brings convenient solutions and it is one of the aims in education (Lankshear & Knobel 2015; Pangrazio 2016; Regeringskansliet 2017 [Sweden]; *Digital India*; Digitaliseringsrådet [several countries]; Børne- og Undervisningsministeriet 2019 [Denmark]; Department for Education 2019 [U.K.]; Federal Ministry of Communication [Nigeria]). The number of internet users is constantly increasing in the world. “Asia and Europe account for double the number of users as compared to the rest of the world combined. Internet penetration in In[dia] and Asia (46%) are considered to be an issue as compared to the economically developed Europe (where it stands at around 80%)” (Bagga-Gupta & Rao 2018). Asia has the highest number of netizens, around three times as many as Europe, and social media sites and use

have grown everywhere (Bagga-Gupta & Rao 2018), which provides an indication of the scope and need for ICT literacy. Moreover, “[s]ocial media has not only become a significant tool for political communication and campaigning in In[dia], but is reported to have also led to a rise in young peoples’ political awareness” (Rahul 2016). It is also reported to have reshaped access to political information (Saleem & McDowell 2016; Bagga-Gupta & Rao, 2018). All this weigh in as more and more countries are working towards their inhabitants becoming proficient users as well as producers of information and communication technologies – in short, ICT literate.

ICT literacy is defined as the ability to use “digital technology, communications tools, and/or networks to access, manage, integrate, evaluate, and create information in order to function in a knowledge society” (Educational Testing Service 2002) and in most countries the socialisation towards an ICT literate population begins in school. For schools within the EU, it may feel safe to have a regulation like GDPR to fall back on to protect student data. Nevertheless, funding is an issue and digital teaching material can be expensive. Education technology is a major investment and hurdle for schools aiming to provide education technology for every student (CLIO 2019). For many schools, 32% in Denmark and 40% in Sweden, Google Chromebooks and Google Education services become convenient and inexpensive solutions (CLIO 2019) and the number of Google Education users is growing. As a part of the shift to emergency remote teaching during the COVID-19 pandemic, the use of Google’s services has escalated as “accounted for ‘60% of the market’ for computers in the education market and the company reported that ‘more than 170 million students and educators worldwide rely on our suite of tools’” (De Vynck & Bergen 2020 and Sinha 2021 in Krutka, Smits & Willhelm 2021). Already in 2017 in the U.S., more than “half the primary- and secondary-school students – more than 30 million children – use Google education apps like Gmail and Docs” (Singer 2017). Is Google Education safe? Google’s large market share has left U.S. parents worried as “[s]chools may be giving Google more than [users] are getting: generations of future customers” (Singer 2017) and, in addition, parents are wary “Google could profit by using personal details from their children’s school email to build more powerful marketing profiles of them as young adults” (Singer 2017). Their fears are legit according to Krutka, Smits and Willhelm (2021): “While Google has largely acquiesced to demands to abide by federal laws, the company has shown a consistent pattern of obfuscating, or even ignoring, their own policies concerning students’ privacy.” In the same vein, Shoshana Zuboff (2019) argues that it is in Google’s interest that such aspects are kept in the dark, since the gathering of non-personal data secures future revenue. Worth noting is that the 2002 definition of ICT literacy

primarily focuses on handling information online, but the above indicates that the evaluation of education technology providers would be equally important to include.

In Europe, Liz Sproat, the head of Google for Education in the region, draws on the adherence to GDPR as she addresses the fears of how student data is being used in the Danish setting:

To make this completely clear: When Google delivers GSuite for Education to schools in Denmark, this happens in accordance with detailed data service agreements. Both GSuite and Chrome operating systems function in accordance with GDPR and thereby safeguard user data. Chromebooks are sold by hardware producers to schools through local retailers and not directly from Google. No commercials are shown in GSuite for Education and data are not being used for commercial purposes. (ITWATCH 2020, *MY TRANSLATION*)

In this case GDPR becomes an alibi for Google. They signal that GDPR as legislation is enough to protect citizens, and, since the company is adhering to the EU regulations, Google has not done anything wrong. Sproat's omission highlights the loophole in the GDPR regulations: she avoids saying anything about the possibility of the company sharing "non-personal information publicly in order to show trends in how our services are being used generally" or how this may influence the children. Since there is no safe-guarding of non-personal data within the EU – quite the opposite, as indicated above – companies like Google can harvest non-personal user data as much as they wish and, as consumers, we give away our rights to the same data when we agree to the privacy notice. In this manner, GDPR provides a smooth space for Google to create revenue from the unregulated non-personal data.

Nevertheless, the sharing of data with third-party interests, which Google states that they do, is indicated as a risk by the organisation Swedish municipalities and regions, a service organisation for Swedish schools. The organisation provides the following advice regarding the selection of education technology: "if we by 'safe platforms' mean various ICT services (learning platforms etc.), an information safety classification needs to be performed. It focuses, for instance, on where information is stored (servers in Sweden, inside/outside Europe, and whether the information is shared by a third party or not)" (Swedish Municipalities and Regions 2019, *my translation*). Following this, the Swedish Municipalities and Regions organisation asks us to question platforms like Google Education, that does indeed "share information publicly" for purposes unrelated to the school or the students in question. This highlights

that school management and teachers may need an extended version of ICT literacy in order to meet the challenges of today's digital context.

Yet another danger, Google could become the gatekeeper of valuable learning or information. In an interview, Jonathan Rochelle, director of the Google's education apps group, is critical towards the contents in his own children's mathematics course (they attend U.S. schools) and says: "I cannot answer for them what they are going to do with the quadratic equation. I don't know why they are learning it." He adds: "[a]nd I don't know why they can't ask Google for the answer if the answer is right there" (Singer 2017). In this case, Rochelle, a senior representative of Google, seems to suggest that a) he, or Google, ought to be able to decide, create striations, whether something is worth teaching or not and b) that learning something in school might become irrelevant, since it is so easy to google to find the correct answer. Both of these issues raise red flags as to what will be considered useful knowledge and learning in future education if the tech companies are to be gatekeepers of such. This notion seems to dispense with the knowledge of how something is done and settles for the "correct answer." As a result, the process of thinking critically and finding your own answers is being made redundant. As Vaidhyanathan (2011) puts it (cited and contextualized in Krutka, Smits & Willhelm 2021): "Google has sought to 'organize the world's information and make it universally accessible and useful,' but this has resulted in problems for democracy and justice." To highlight this, perhaps in an extreme manner: Is American education, or education throughout the entire world since Google operates on a global scale, supposed to produce knowledgeable, democratic citizens, who can reason their way to an answer, or skilled workers (Singer 2017), who focus only on doing what they are set to do without questioning? "Unfortunately, democratic and just aims can also conflict with profit-motives" (Krutka, Smits & Willhelm 2021). Will the world allow companies like Google to become the gatekeepers, those who decide on the framework and focus, striations, in education? Google is not the only company to take on a gatekeeping function or to take advantage of their users' non-personal data to gain sellable data, but, since the company is specifically targeting children through some of their services and has such a large market share, they are worthy of some scrutiny.

This section illustrates how the negotiation of power, striation vs. smoothness, is a continuous part of new technology. For whom does it become smooth and from what perspective, though? A company like Google creates a service, and, while being useful to the users, it logically also has inbuilt features intended to create revenue for the company. Users begin to use it, not always seeing more than the benefits to them as users. "Google has infiltrated schools by taking advantage of schools' 'dual ambition' to improve technology and cut

budgets by offering free software and inexpensive hardware (Lindh & Nolin 2016). The company then profits from students' personal data and brand loyalty among teachers (e.g., Google Certified Educator) and students" (Krutka, Smits & Willhelm 2021). Organisations such as the EU or, on a smaller scale, the Swedish Municipalities and Regions, discover potential dangers to citizens and introduce laws and regulations, striations, which diminish the freedom of the tech company and may lower the profits, while empowering the users – they are indicating another aspect of ICT literacy focusing on data ownership, profit, and potential misuse – but this is a comparatively new field. Loopholes remain and negotiation of power continues. The main question is whether the striations and the smooth areas are intended to be beneficial for the users or for the tech companies and to what extent their striations are cloaked in what seems smooth to a user.

Personal Versus Non-personal Data and the Commodification of Users

The wording in the Google Education privacy notice and Liz Sproat's comment above stresses that Google abides by the European Union GDPR (and the laws in many other countries) as it promises to secure personal data, but, as indicated, the last sentence in the quote from the privacy notice – "we might share information publicly in order to show trends in how our services are being used generally" – also delineates the smooth space facilitating the company's data harvesting from anyone using Google's services. The company continues to trade in non-personal data since this remains a smooth, unregulated area in which they can continue to make profit. As a result, users are turned into commodities. "Commodification is a term that is being used to describe the transformation of something, a good or a service that does not have an exchange value, into a commodity, into something that can be bought and sold on the market" (Wittel 2013). In this way, user information can be bought and sold to gain knowledge, for instance, of general preferences and values in a society. The knowledge about the values of an individual or a group of individuals (be it conservative or liberal or in any other direction) could be used for prodding people towards more entrenched political positions using the dissemination of selected facts – facts that may be true or false. In March 2018, news of the Facebook-Cambridge Analytica data scandal broke and alerted many people to the dangers of their data being used in ways they did not anticipate, linking Cambridge Analytica to potential voter fraud in the 2016 U.S. presidential election as well as in the same year's U.K. referendum to leave the EU (Confessore

2018). At that point, it became clear that the harvesting and selling of user data could be used to chart and (perhaps) influence attitudes in society. The secret smooth space, which had been created by the global tech companies, became public and it became obvious that companies like Facebook and Google gain a substantial amount of their revenue from behavioural data generated “for free” by the users of their services (Simanowski 2018; Travizano 2018; Zuboff 2019; Krutka, Smits & Willhelm 2021). As such, they were transformed from neutral service providers to cloaked actors in the eyes of the public.

The Facebook-Cambridge Analytica data scandal generated interest in many parts of the world, but the shockwaves ran especially high in Europe and North America, where a large portion of people had access to high-speed internet and used Google and Facebook on a daily basis. This is not the only geographical sphere of interest for the two companies. They also

have sought to expand their reach in developing countries in the Global South. These emerging markets present Facebook and Google with lucrative opportunities for growth, largely through the potential for expanded access to data. The Free Basics service is another way in which Facebook can collect masses of data from people in developing countries. According to a recent UN report, “For advertising platforms, such as Google and Facebook, more (local) data would mean opportunities for providing better, targeted advertising...With Facebook’s Free Basics, traffic is effectively channelled through a portal, reflecting the reliance of Facebook’s business model on a more closed platform.” In its response to this report ... Facebook asserts that “Free Basics does not store information about the things people do or the content they view within any third-party app.” (AMNESTY INTERNATIONAL)

Facebook’s Free Basics was intended to become the new frontier, another smooth space, where Facebook could create striations for the users in a manner that suited them and generated revenue. Of particular interest may be the last part of the above quote, as it indicates that they do not store content within third-party apps, but they do not say anything about the type of content they store generated in their own app.

As the number of people with internet access has grown in what is referred to as the Global South, connectivity as well as ICT literacy issues remain in many countries, for instance India, as Prasad Banerjee (2018) and *Digital India* indicate. This has hampered Google in their quest to launch their Chromebooks on a large scale, as these require constant internet access. Facebook has, with

the abovementioned Free Basics app, attempted to become a player on a market with shaky internet access by making it possible for users to “connect to Facebook and other websites for free using a SIM card from a qualifying mobile operator. Stay in touch with friends and family, search for jobs, check out news and sports updates, and get health information – all without data charges” (Google Play). Through this portal, users can access websites such as AccuWeather, BBC News, Facebook, Dictionary.com, UNICEF (Google Play) and, according to the description, Facebook works with “mobile operators around the world to make Free Basics widely available” (Google Play). This may sound positive, but in a 2017 article in *The Guardian*, Free Basics is accused of “digital colonialism” (in this case a digital tool imbued with a colonial mindset, and as such inherently disrespectful of its intended users) and is described as being primarily focused on ‘western corporate content’ and accused of violating net neutrality principles (Solon 2017). In a report published by the organisation Global Voices, a global anti-censorship network/NGO of writers, bloggers and activists dedicated to protecting freedom of expression online, the authors conclude that

[s]imilar to an internet service provider, Facebook’s Free Basics program collects metadata about *all* user activities, not just the activities of users who are logged into Facebook... [It also] offers access to a small set of services and prioritizes the Facebook app by actively urging users to sign-up for and log into the service. Free Basics also divides third-party services into two tiers, giving greater visibility to one set of information over another. (GLOBAL VOICES)

Again, this underlines that this is a very important source of profit for companies like Facebook, that the harvesting of this type of data is well integrated in their business model, and that they are willing to adapt their services to establish themselves in previously – by them – untapped markets in an attempt to gain a market share that can be expanded with time. More non-personal user data will lead to increased revenue. In other words, Facebook’s Free Basics is not truly free since users are paying with their own data and, if users wish to get access to more of the internet than Facebook has walled off as free, this will also cost them in money. Hence, from a user perspective, Free Basics could be described as a supposedly smooth space with hidden striations for the user beneath the surface. By creating Free Basics, Facebook is again using the division between personal and non-personal data to create revenue at its users’ expense.

The Dichotomised Relationship Between the Digital Global South and Global North

Facebook's Free Basics highlight three aspects, which in effect function as striations on the users, from a report written by the organisation Global Voices with a focus on the effects of digital colonialism. Firstly, the number of languages available do not reflect the linguistic needs of the countries where they launch First Basics. By not meeting "the linguistic needs of target users," the app may not "adequately [serve] the linguistic needs of the local population. In heavily multilingual countries... the app is offered in only one local language" (Global Voices). This excludes many people from using it, although it may not be a Global South and Global North issues per se. This perspective on local languages stresses the idea that every nation-state only uses one main language; that every country is monolingual within its borders. If viewing Free Basics as a mediascape (a digital, multi-media region lacking physical borders where people can interact) where users operate in many different countries, Facebook does not seem to understand the multifaceted nature of their users, or, if they do, they wish them to conform to fit their business model. This ties to Bagga-Gupta and Rao (2018: 28):

[S]uch mediascapes, unlike the constructed boundaries that demarcate one nation-state from another, are not hermeneutically sealed spaces; they are part of the larger medial landscapes, including societal contexts. The internet allows anyone with a technological device and a connection, including a desire to connect with anyone else with similar connectivity, to connect. Here language has been and continues to be an issue – particularly in terms of access to the "multilingual internet" (Crystal 2011: 78–91)... the new media situation across GSN [Global South-North] settings cannot be simplified to an issue of haves-have-nots.

The basic assumption of Facebook's Free Basics is that internet is supposed to be "given" to those without access. At the same time, Facebook does not seem to appreciate the complexities related to pushing a homogenised, striate solution on a heterogeneous world. Secondly, the app also

features an imbalance of sites and services. All versions we tested lacked key local content and services, but featured a glut of third-party services from privately owned companies in the United States. Apart from services that are owned and/or operated by Facebook, the versions of Free Basics that we tested included none of the world's 15 most popular

social communication platforms, nor did they include an email platform.
(GLOBAL VOICES)

This highlights one of the inherent aims of the app: to create business for American companies, which, again, points to a striate, homogenised solution, which limits users. Thirdly, Free Basics also limits their users by not allowing them “to browse the open internet,” but to force them to stay within the limited range of websites selected by Facebook (Global Voices), which constitutes a third striation. These three aspects are ultimately linked to Facebooks dwindling credibility in the Global South, which draws attention to the company’s dichotomised view of those without digital access in this region and their idea of how to take advantage of this, in their eyes, deficiency.

In a Guardian article, author Cory Doctorow (2016) calls Free Basics a “poor internet for poor people” and points out that the rhetoric around the concept “the next billion users”, of which Facebook’s Free Basics is a part, seems extremely seductive for the global tech companies. Under the cloak of “doing good through tech innovations” they attempt to create a smooth space rhetorically intended to empower people in the Global South, but the definition of “doing good” is theirs, not their presumptive customers’. In this, Facebook continues “a long legacy of wealthy nations, international corporations, and aid agencies” in their wish to “help the poor ‘leapfrog’ their way to a better life, the ultimate self-help solution to global inequality” (Arora 2019) through the use of mobile technology. For these interests,

poverty is an opportunity and scarcity is a resource; the poor are the experts in leveraging mobile apps to get a better life for themselves, if we are to believe this narrative. While investing in these “next billion users” started as supposed altruism decades ago, today it is a critical business strategy for technology companies. It is no surprise that in 2018 alone, numerous symposiums, initiatives, labs, and products have been launched to target these users. Leading the pack is Google with its Next Billion User (NBU)¹ Market division. (ARORA 2019)

The above quotes show the business opportunities for the global tech corporations and they also exemplify how invested both Facebook and Google are in the Next Billion User idea. Although the rhetoric may sound seductive, it draws the attention to a matter of utmost significance: the fact that most infrastructure that has become vital all over the world may be in the hands

1 Google Next Billion Users, <https://www.blog.google/technology/next-billion-users/>.

of privately-owned corporations from countries far away from where they operate. As indicated above, these companies have their own agendas, their own reason for wanting to increase their market share, their own reasons for gathering information, and their own reasons for turning their users into commodities. Although digitisation is experienced as a positive development and many countries aspire to a high level of ICT literacy in their countries, it has also brought down-sides:

Digitalization generally and Web 2.0 platforms specifically have changed not only engagement patterns, but also how democracy plays out in everyday life (Narayan and Narayanan 2016). While participation is contingent upon access to digitalization tools in a very tangible sense, issues of engagement do not follow a linear, foreseeable, developmental trajectory. Such issues of access and participation have seen the emergence of an interest in the study of alternative digital political spaces (Schroeder 2016); here affinity spaces are potentially open for politicians, citizens and political parties, anywhere 24/7. This does not mean, however, that openness automatically results in universal access or inclusiveness. Openness implied in digitalization is simplistic and reductionist and technology cannot be viewed as an agent that makes individuals, institutions or nation-states more democratic. Given that technologies have “implications for patterns of sociality” (Ingstad and Whyte 2007: 20), it is necessary that research recognizes both the affordances and constraints that digitalization gives rise to. (BAGGA-GUPTA & RAO, 2018: 5)

Aspects of access, participation, openness, and inclusiveness must be balanced with notions of security and trust. The choices of what technology or which supplier to trust could impact the very fabric of a country and affect democracy – which can become an issue regardless of where this country is situated in the world. Those who own the information and control the supply chain of information, i.e. create striations for others, are a position to rule the world and can only be held accountable if their strategies are made publicly known, discussed, and, if need be, limited.

Online Security and Issues of Trust

So far in this paper, Google and Facebook have been in focus for exploiting their users for profit, but users may be taken advantage of in other ways. The above-mentioned Facebook/Cambridge Analytica data scandal is such an

example, in which user data was used for political gains. This section broadens the focus and addresses the impact of similar technical solutions implemented by companies, but sometimes also by countries, in their efforts to gain access to user data not only for profit but also for the authoritarian control of citizens.

When digital tools are used in line with democratic frameworks from the perspective of protecting and providing benefits for users in accordance with regulations and in line with human rights, users often take for granted that this usage is benign and safe. They might also take the protection against commodification or other types of malicious data mining for granted. In a world controlled by the global tech companies, they are not always secure, however. One example is the Huawei backdoor scandal, which involved so-called hidden backdoors in the software found in the Italian Vodaphone phone system. This opened up for Chinese Huawei, who had provided some of the software, and potentially also the Chinese government (since Chinese companies must allow the government access to any information they have), to gain access to user data without Vodafone's knowledge (Lepido 2019). As a result, Italian user data might have been shared with the Chinese government. Would an Italian user trust the Chinese government and, if not, what could they do about it? The powerlessness in this type of situation is tangible.

The importance of trust, strongly underlined by Lysne, is foregrounded: "The trustworthiness of electronic equipment is paramount and we cannot choose to design and produce all aspects of this equipment ourselves. The question we then need to answer is how we can check and verify the equipment and how we can build well-founded trust" (2018). Lysne contends that countries with undemocratic, highly authoritarian regimes – he uses the Huawei backdoor scandal as an example – are less trustworthy than their democratic counterparts. Ma & Yamin (2020) also highlight countries, where the population may be supervised and controlled through the use of data mining and where national security primarily means security for the leaders, as less trustworthy than countries with liberal democratic ideals.² The underlying assumption is that the majority of citizens in well-functioning, democratic nation states benefit from societal and industrial development, whereas only a small minority may benefit from the same in countries with undemocratic leaders. In line with this argument, trust between people and between groups of people in democratic countries ought to be higher than in undemocratic and/or corrupt ones, where prosperity and wealth might be distributed among

2 Democratic governance is here characterised by free elections, individual inhabitants' rights, freedom and responsibilities, and a division of power between politicians, legislators, and heads of state, where national security is supposed to safeguard everyone equally.

a few. In democratic countries, the idea of a digital smooth space – without risk of being taken advantage of and without surveillance – is the self-evident norm for most users. From the perspective of global tech companies, digital smooth space is first and foremost intended for their companies. For authoritarian regimes, digital smooth space is primarily intended for the leaders of that regime. So, depending on the system at hand, who can be trusted? Who benefits from the data gathered by technological solutions? For whom is a smooth space intended?

As examples of how a country can take a stand against both global tech corporations and foreign nations, the following two examples are taken from an Indian context. In February 2016, Telecom Regulatory Authority of India (TRAI) takes a stand against Facebook and Free Basics as the ruling Telecom Regulatory Authority of India (2016) is published on their website. The authority argues that in order to “preserve the unique architecture of the Internet as a global communication network” (Telecom Regulatory Authority of India) they need to secure against

[p]rice-based differentiation [that] would make certain content more attractive to consumers resulting in altering a consumer’s online behaviour. While this might not be a major concern in a country where the majority already has Internet access, in a nation like India which is seeking to spread Internet access to the masses, this could result in severe distortion of consumer choice and the way in which users view the Internet. (TELECOM REGULATORY AUTHORITY OF INDIA)

It is therefore necessary to limit differentiation in terms of internet access, since they need “to ensure that service providers continue to fulfil their obligations in keeping the internet open and non-discriminatory” (Telecom Regulatory Authority of India). Although the crackdown on “price-based differentiation” may seem like an insignificant detail, this verdict stops Facebook’s strategy for rolling out the aforementioned Free Basics in India, as their portal service relies on added fees on all that is outside of their free basic service (*The Indian Express* 2016). Hence, Facebook has lost the trust of Indian authorities. They counter Facebook’s advances by exposing the hidden striations in the company’s strategy, which were intended to ensure revenue in India. Instead, this becomes the key to the failure of the Free Basics endeavour in India.

As seen above, Indian Telecom Regulatory Authority primarily wishes the internet to remain “open and non-discriminatory” and is willing to go to great lengths to keep it so, but Indian authorities also take a stand against other nations. The second example is from late June 2020, as the violent clashes

between Chinese and Indian soldiers on their joint, but contested, border leads to Indian authorities banning 59 Chinese-owned apps. These apps are considered “prejudicial to sovereignty and integrity of India, defence of India, security of state and public order” (BBC News 2020) indicating that Indian authorities are wary of Chinese involvement and espionage. The trust between the two countries is broken, to use Lysne’s term, and, in an act of resistance intended to smooth out striations imposed by the other, India stops Chinese companies from gaining revenue or to benefit from non-personal data in India. As such, India creates striations for China.

This decision is not necessarily applauded by Indian users, as one of the banned apps is the popular TikTok. Its user base has grown rapidly in India and brought fame and a new sense of agency and adventure, provided a smooth space, for people like Gaikwad, who did not anticipate this:

Gaikwad [was] growing up poor in Maharashtra state and raising four children with Ankush, who earns \$120 a month as a local government employee. When she goes to the market now... people stop her for selfies. Strangers ask to shoot videos with her. Some even come to her house. “I never got into TikTok for money,” she said. “But I got respect, legitimacy and confidence. We are poor people. We have never received any attention in life. All we have gotten is disdain and scorn. TikTok turned it around.” (SHASHANK BENGALI, 2020)

Similar stories are told in other newspaper articles and many users mourn the banning of TikTok:

“TikTok was easy and a home for marginalised sections like us. We felt like home on TikTok. Other apps like Instagram are complicated. Nobody cheers us on other apps like the users on TikTok appreciated us. We can’t imagine big people writing about us if it was not for TikTok,” said Chavan. (YADAV)

This highlights the need to be seen, heard, accepted, and liked – in effect, to experience a sense of agency – a need shared by many people all over the world. This is a strong reason why people may wish to continue using apps such as these even if the authorities deem them unsafe or unsuitable on individual as well as national levels. TikTok has provided a smooth space for users like Gaikwad and Chavan, but individual users may not realise that the gathered data is shared by companies and/or governments and has the potential to impact negatively on societies from a democracy and human rights perspective

(Gehl 2014; Harcourt 2015; Hayles 2016; Cheney-Lippold 2017; Mau 2017; Salganik 2017; Pötzsch 2018; Simanowski 2018). Since these digital solutions are so ubiquitous, questions of agency, transparency, dissemination of learning and power must be asked. Individuals must learn to ask questions. Who can be trusted? Do developers create striations for users in order to protect their own agency or smooth space? Are their actions compatible with democratic values and human rights? Could users of digital services, or the authorities on their behalf, take a stand and subvert the striations imposed by undemocratic or inhumane owners if need be or are they too powerful to be affected?

What can be Done?

In this paper, I have pointed to several examples of how online exploitation and commodification have been subverted. The “obligations in keeping the internet open and non-discriminatory” are guiding the Telecom Regulatory Authority of India, which highlight the potential of subverting striations imposed by the global tech companies in favour of an open, egalitarian and democratic positioning towards the internet, viewing the internet as a smooth space for *users*. The sources above express similar aims and highlight negative aspects of digital ownership, marketing and use, where global tech companies could be viewed as taking advantage of their users. The perspective of the authorities, legislators, researchers, and journalists builds on the idea to safeguard human values and individual citizens. To be guided by these values is fundamentally a choice based on education, regardless of this being on an individual or societal level.

As things currently stand, corporations such as Google and Facebook harvest non-personal user data in the smooth, unregulated space of technological novelty and innovation. Authorities and legislators need time to catch up and formulate rules and regulations in order to protect the citizens. As the examples above have indicated, this has happened in the EU as well as in India, and there are many more nations with the same or similar aims. A focus on other countries and regions would no doubt have elicited other examples, which the paper’s primary focus on the EU and India may hide, but there may also be similarities. However, in dictatorships or countries with dysfunctional democratic systems, authoritarian values or interests may be prioritised. No doubt, the difference between the value systems of individual nation states and/or companies will cause clashes now as well as in the future. The battles may not be fought with soldiers and conventional weapons in conventional wars. Instead, the weapons may be information/disinformation, financial embargos,

the blocking of websites, apps, and software or anything else that carries political weight in that particular situation or relationship.

This fight can be similar on an individual level. In the government-inhabitants relationship, citizens may accept limitations on their freedom if they perceive that these are supported by valid reason or if they gain something in return. To illustrate this, I am drawing on yet another example from India and the banning of TikTok:

Even among ardent TikTok users, there has been little pushback to the ban, widely seen as a necessary response by Modi's Hindu nationalist party to Chinese aggression.... "Given that soldiers have been killed and sentiments are running high, banning Chinese apps is going to be a popular move," Pahwa said. "What we see are people looking for alternatives. If the situation doesn't get resolved over the next month, creators will have to find other platforms to migrate to." (SHASHANK BENGALI, 2020)

As indicated above, apps like TikTok empower users. In the perceived or real rigidity of their daily lives, users gain freedom and joy from being creative, becoming seen and heard, and interacting with people online. In using TikTok in such a manner, these individuals create a smooth space for themselves. Nevertheless, tensions may arise between that, which we find amusing online, and the understanding that we need to deal with internet critically. As Roberto Simanowski (2018) puts it: "Most of what would be good for the formation of political opinions is detrimental to business – complex reflexion instead of amusing banalities, unsettling instead of affirmative views, criticism and scepticism instead of sensation and dopamine" (*my translation*). Citizens are supposed to contribute and become educated in fields deemed important by the authorities – for instance digitisation – and understand the complex reasons behind decisions made by the authorities – as well as those decided on by the tech companies. Within the striations of our societies, its laws, regulations, expectations and conventions – online or offline – we may create joint as well as individual smooth spaces, where there is freedom to play or to experience stimulating interaction and communication. Simultaneously, the same regulations may also create striations stifling this experience of freedom. In order for balance to be achieved or maintained, a shared goal and trust between leadership and people is required. Are we in agreement with the priorities made by governments? Can we see the benefits? Would we rather side with Google's Jonathan Rochelle arguing a more utilitarian stance? Discussion is free. The freedom of citizens may also be limited by the decisions of the global tech corporations. To pull this line of reasoning a bit further, do we understand the

reasons behind decisions made by the tech companies? Can users influence these? How are shared goals and trust maintained in this unequal power structure? The most important conclusion might be that governments can be voted away. Companies cannot.

Parts of the push for knowledge, *Bildung*, in the field of digitisation are related to the above (Simanowski 2018). Simanowski argues that technical know-how ought to be a part of *Bildung*, the general knowledge, in society. As several of the national development plans indicate: citizens need to learn how technology works, be able to explore it, use it, understand it, and develop it. Citizens must be knowledgeable enough to make the most of these tools, but they also need to be able to recognise misuse. Citizens must be able to ask questions such as “why is this service free?” and “who gains from my participation?” To foster this type of awareness – to draw computerised services out of invisibility – is important from a democratic perspective. The role of education in this area may be to highlight that there is no such thing as a free lunch. There is almost always a cost and if citizens are well educated, they may spot this. In this paper, global tech company ownership is in focus, but, simultaneously, issues of democracy, the freedom to choose, the obligation to keep the internet open and non-discriminatory are foregrounded. Education can make people understand the importance of supporting organisations and authorities trying to protect inhabitants unable to stand up to large corporations or unjust governments on their own. Education allows people to scrutinise the authorities *and* to examine corporations like Google and Facebook when their deal seems to be just a tad too sweet. Control of information, knowledge and learning becomes an issue of power. Commodification could be seen as a homogenizing tool used on users to take away their control, whereas global tech company leadership will retain theirs. This hampers diversity as well as democracy, as it leads to the streamlining of information and knowledge. Should companies like Google and Facebook have that power? Should foreign governments have that power? Subversive tactics, underpinned by widely disseminated societal and technical know-how, can be the tools to move beyond the uneven power hierarchy sketched here.

Conclusion

Using Gilles Deleuze and Felix Guattari’s concepts of smooth and striate space allows us to analyse power in flux and to identify the striations imposed on others, in this case often on the users of digital services, by the global tech companies. Although many of their services are “free,” the analysis of the texts

in this paper has highlighted that users pay with their habits, search results, and anonymised information, which can be used to predict the behaviour of a large number of people, something which has become their main source of revenue. The analysis has also shown how authorities, on behalf of the users, have succeeded in subverting the control and hierarchic power of the global tech companies, introduced smooth spaces and shown that this is indeed a possibility for resistance against commodification.

So far, Google and Facebook, and companies like them, have exploited the unregulated, smooth space of the internet, where they are not stopped from pursuing their goals to create revenue. Currently, they are in power and non-personal data is completely in their hands. A related issue concerns a foreign government's access to user data. In the power struggles between countries, private user data may become hard currency and an efficient way of gathering information about, for instance, political leanings in an enemy nation. It may also show a way to influence an enemy population, spread misinformation or negatively affect morale. Globalisation has facilitated the spread of apps, search engines, and websites. Algorithms are making some of them more popular and more pervasive than others. Again, who controls them and what is their purpose? This is yet another aspect where countries must work together on an international level, lift the issue more broadly and introduce striations to safeguard users. Striations on one level, for instance between countries, with the aim to reconcile different political, legal or regulative stances can, somewhat contradictory, be used to introduce smooth space for individual citizens on another. For example, if striations are used to keep authoritarian regimes and their hierarchic control apparatus in check, their people can perhaps become freer and experience increased agency and purpose. Is leadership supposed to have agency and freedom at the expense of the population or should there be mitigating measures spreading the power, agency and freedom more evenly? At the core of it all lie concepts like human rights and democracy, which may look different in different countries and cultures. Nevertheless, just like technology, they must be pulled from invisibility.

Again, questions need to be asked. Who has agency? Is there transparency? Who controls the dissemination of learning and what is being taught? Who has power? "Who knows? Who decides? Who decides who decides?" (Zuboff 2019). What are the aims and values behind legislation, and who has the power to information? Is power in the right hands? It may be possible to resist commodification and the misuse of user data through the teaching about, and legislation of, these aspects. It is not self-evident that companies like Google and Facebook should remain in power and, as Simanowski indicates, education and legislation are our tools to subvert this power. Power – in this as in other

fields – can and should be negotiated and, when the need arises, subverted. Smooth and striate go hand in hand. What appears smooth for one is a limiting striation for someone else. Matters shift and change. Hierarchies may crumble and be replaced by something new. What used to be open, anti-authoritarian and flexible, such as the internet during the 1990s and early 2000s, has become more controlled, hierarchic and regulated. People expressed feeling unsafe, which pushed legislators and the global tech companies towards striations, but the different players have made alterations for different reasons and sometimes also in different directions. Legislators have tried to balance the profit-oriented demands of the companies with the interests of the users. In the EU, and in countries like India, Brazil, and Nigeria, the rights to personal data have been secured while at the same time allowing companies enough leeway to make money. Tech companies create revenue, which usually is no problem, but as these companies have grown and achieved a monopoly status in many parts of the world, their power sometimes becomes bigger than that of governments, which leads to a conundrum, since, as mentioned above, companies cannot be voted away. The tools and weapons to shift power from the global tech companies to the users are legislation and education, which requires an enhanced ICT literacy, incorporating not only the use of digital tools but an awareness of the forces behind the tools and a knowledge of the dimensions of power present in the field.

As indicated by the authors of the various texts referred to in this paper and while computers and computerised services are becoming more and more self-evident as tools – and therefore also increasingly invisible to the general user (Simanowski 2018) – an increasing number of researchers, journalists, legislators, and authorities are trying to find ways to combat digital threats against individuals and society, while encouraging the usage and maintenance of an open internet. These categories of people may have differing reasons for doing so, may articulate their visions in ways that may not be immediately decipherable to each other or to users in general, but they are all a part of the multitude of voices that communicate via the internet about the internet.

Human communication is always messy and its study always entails challenges, both from analytical and methodological perspectives. Its complexity and messiness need recognition as the norm, rather than something that needs to be fixed for others. We propose, in all its triviality and mundaneness, that there is merit in fixing our analytical gaze at the meaning-making of participants, irrespective of how many language-varieties/modalities and other resources they deploy. Such an enterprise necessitates that we analysts ourselves share those meaning-making

resources, if we are to avoid contributing to Othering processes, including sloganism within scholarship. (BAGGA-GUPTA & MESSINA DAHLBERG, 2018: 405)

The voices from the various sources in this study highlight similarities in the discourse on user-generated data, commodification, and echo similar fears regarding their negative impact on democratic societies and human rights. These voices express these through the channels they have at their disposal, be it newspaper articles, laws, academic reports or government policies. With a common interest in opposing user commodification in the digital realm, they act, attempt to create a smooth space, to counteract the striations imposed on individuals, communities, and countries by the global tech companies. Knowledge is power and, subsequently, widely disseminated knowledge ought to lead to more widely disseminated power as it might be, at least partially, wrested out of the hands of the tech companies and empower users.

Compared to when the research for this paper began, there are now many articles as well as fictional and documentary films addressing data ethics, the effects of data harvesting and Big Data. The articles are often bound to disciplinary frameworks, however, and may focus on public discursive practices, politics, legal issues, education, discrimination, business, public health (especially pandemic-related aspects), and media practices. Few are attempting a more holistic approach, which would be an interesting line of enquiry for future research.

References

- Amnesty International. 2019. *Surveillance Giants: How the Business Model of Google and Facebook Threatens Human Rights*. London: Amnesty International.
- Arora, Payal. 2019. "The biggest myth about the next billion internet users." *Quartz*. November 5, 2019.
- Bagga-Gupta, Sangeeta, and Giulia Messina Dahlberg. 2018. "Meaning-Making or Heterogeneity in the Areas of Language and Identity? The Case of Translanguaging and Nyanlända (Newly-Arrived) across Time and Space." *International Journal of Multilingualism* 15 (4): 383–411.
- Bagga-Gupta, Sangeeta, and Aprameya Rao. 2018. "Languaging in Digital Global South–North Spaces in the Twenty-First Century: Media, Language and Identity in Political Discourse" *Bandung: Journal of the Global South*. 5 (1): 1–34.

- Banerjee, Prasad. 2018. "Why Google Chromebooks Aren't in Favour In India." *Livemint*. September 21, 2018.
- BBC News. 2020. "India Bans TikTok And Dozens More Chinese Apps." *BBC News*. June 29, 2020. URL: <https://www.bbc.com/news/technology-53225720>.
- Blog Google. "Next Billion Users." Accessed July 11, 2020. URL: <https://www.blog.google/technology/next-billion-users/>.
- Børne- og Undervisningsministeriet. 2019. "Om Kampagnen "Digitalisering Med Omtanke Og Udsyn"." January 1, 2019. URL: <https://www.uvm.dk/publikationer/2019/190313-digitalisering-med-omtanke-og-udsyn>.
- Cheney-Lippold, John. 2017. *We Are Data*. New York: NYU Press.
- CLIO. 2019. "Digitization in Swedish Schools 2019." *Clio*. January 1, 2019. URL: https://www.clio.me/wp-content/uploads/2019/08/se-market-research-2019-main-conclusions-report.pdf?utm_source=SE_BrandSite&utm_medium=Blog&utm_campaign=SE+Market+Research+2019.
- Confessore, Nicholas. 2018. "Cambridge Analytica And Facebook: The Scandal And The Fallout So Far." *The New York Times*. April 4, 2018. <https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html>.
- Crystal, David. 2011. *Internet Linguistics*. London: Routledge.
- Curran, D. 2018. "Are you ready? Here is all the data Facebook and Google have on you." *The Guardian*. March 30, 2018.
- Cyphers, B. 2020. "Google Says It Doesn't 'Sell' Your Data. Here's How the Company Shares, Monetizes, and Exploits It." *Electronic Frontier Foundation*. March 19, 2020.
- De Vynck, G. & Bergen, M. 2020. "Google Classroom users doubled as quarantines spread." *Bloomberg*. April 9, 2020. URL: <https://www.bloomberg.com/news/articles/2020-04-09/google-widens-lead-in-education-market-asstudents-rush-online>.
- Deleuze, Gilles, and Félix Guattari. 1986. *Nomadology*. New York, USA: Semiotext.
- Department for Education. 2019. *Realising the Potential for Technology in Education: A Strategy for Education Providers and the Technology Industry*. London, U.K.: Department for Education. Accessed July 11, 2020. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/791931/DfE-Education_Technology_Strategy.pdf.
- Digitaliseringsrådet. n.d. "Andra Länders Digitala Strategier." Accessed July 11, 2020. URL: <https://digitaliseringsradet.se/vaerldens-digitala-agenda/andra-laenders-digitala-strategier/>.
- DLA Piper. n.d. "DLA Piper Global Data Protection Laws Of The World." Accessed July 11, 2020. URL: <https://www.dlapiperdataprotection.com/>.
- Doctorow, Cory. 2016. "'Poor Internet For Poor People': India's Activists Fight Facebook Connection Plan." *The Guardian*. January 15, 2016.

- DuBois, Andrew. 2003. "Introduction." In: Frank Lentricchia and Andrew DuBois 2003. Eds. *Close Reading: The Reader*. Durham: Duke University Press.
- Educational Testing Service. 2002. *Digital Transformation: A Framework for ICT Literacy* (A Report of the International ICT Literacy Panel). Princeton, New Jersey: Educational Testing Service.
- European Commission. 2020a. "Shaping Europe's Digital Future. Policy. Free flow of non-personal data." *European Commission*. October 2, 2020. URL: <https://ec.europa.eu/digital-single-market/en/free-flow-non-personal-data>.
- European Commission. 2020b. "A European Strategy for Data." *European Commission*. September 30, 2020. URL: <https://ec.europa.eu/digital-single-market/en/policies/building-european-data-economy>.
- Federal Ministry of Communication. n.d. "Nigeria E-Government Master Plan." URL: <https://www.commtech.gov.ng/Doc/NgeGovMP.pdf>.
- Fussell, S. 2019. "Google's Totally Creepy, Totally Legal Health-Data Harvesting: Google is an emerging health-care juggernaut, and privacy laws weren't written to keep up." *The Atlantic*. November 14, 2019.
- GDPR.EU. n.d. "What Is Considered Personal Data Under The EU GDPR?" GDPR.EU. Accessed July 11, 2020. URL: <https://gdpr.eu/eu-gdpr-personal-data/>.
- Gehl, Robert W. 2014. *Reverse Engineering Social Media*. Philadelphia: Temple University Press.
- General Data Protection Regulation (GDPR). "General Data Protection Regulation (GDPR) – Official Legal Text." GDPR.EU. Accessed July 11, 2020e. URL: <https://gdpr-info.eu>.
- Global Voices. 2017. Free Basics in Real Life: Six Case Studied on Facebook's Internet 'On Ramp' Initiative from Africa, Asia and Latin America. Amsterdam: Stichting Global Voices.
- Google Play. "Free Basics By Facebook – Appar På Google Play." Accessed July 11, 2020c. <https://play.google.com/store/apps/details?id=com.freebasics&hl=sv>.
- Google G Suite. "G Suite Terms Of Service – G Suite." Accessed July 11, 2020d. URL: https://gsuite.google.com/terms/education_privacy.html.
- Harcourt, Bernard E. 2015. *Exposed*. Cambridge: Harvard University Press.
- Hayles, N. Katherine. 2016. "Cognitive Assemblages: Technical Agency and Human Interactions." *Critical Inquiry* 43 (1): 32–55.
- The Indian Express. 2016. "TRAI Supports Net Neutrality, Effectively Bans Free Basics: All That Happened In This Debate." February 9, 2016. URL: <https://indianexpress.com/article/technology/tech-news-technology/facebook-free-basics-ban-net-neutrality-all-you-need-to-know/>.
- Ingstad, Benedicte, and Stephen Reynolds Whyte. 2007. *Disability in Local and Global Worlds*. Berkeley: University of California Press.
- ITWatch. 2020. "Sager Om Brud På Elevers Datasikkerhed Hober Sig Op." January 31, 2020. URL: <https://itwatch.dk/ITNyt/Brancher/Sikkerhed/articlen191365.ece>.

- Krutka, D. G., Smits, R. M. & Willhelm, T. A. 2021. "Don't Be Evil: Should We Use Google in Schools?" *TechTrends*. 65: 421–431.
- Lankshear, Colin, and Michele Knobel. 2015. "Digital Literacy and Digital Literacies: Policy, Pedagogy and Research Considerations for Education" *Nordic Journal of Digital Literacy*. 10 (1): 8–20.
- Lepido, Daniele. 2019. "Vodafone Found Hidden Backdoors in Huawei Equipment." Bloomberg. April 30, 2019.
- Lindh, M., & Nolin, J. 2016. "Information we collect: Surveillance and privacy in the implementation of Google apps for education." *European Educational Research Journal*. 15(6), 644–663.
- Lysne, Olav. 2018. *The Huawei and Snowden Questions: Can Electronic Equipment from Untrusted Vendors be Verified? Can an Untrusted Vendor Build Trust into Electronic Equipment?* Cham: Springer Open.
- Ma, Jinsong and Mohammad Yamin. 2020. "5G Network and Security," In: 2020 7th International Conference on Computing for Sustainable Global Development (INDIACom), 12–14 March 2020, New Delhi, India. URL: <https://doi.org/10.23919/indiacom49435.2020.9083731>.
- Mau, Steffen. 2017. *Das Metrische Wir*. Berlin: Suhrkamp Verlag.
- Pangrazio, Luciana. 2016. "Reconceptualising Critical Digital Literacy." *Discourse: Studies in the Cultural Politics of Education*. 37 (2): 163–74.
- Pöttsch, Holger (2019). "Critical Digital Literacy: Technology in Education Beyond Issues of User Competence and Labour-Market Qualifications." *tripleC* 17(2): 221–240. <http://www.triple-c.at>.
- Rahul, K. 2016. "Use of New Media in Indian Political Campaigning System." *Journal of Political Sciences & Public Affairs*. 4(2): 1–7.
- Regeringskansliet. "Regeringen Beslutar Om Nationell Digitaliseringsstrategi För Skolväsendet." Accessed July 11, 2020h. URL: <https://www.regeringen.se/informationmaterial/2017/10/regeringen-beslutar-om-nationell-digitaliseringsstrategi-for-skolvasendet>.
- Saleem, Awais, and Stephen D. McDowell. 2016. "Social Media and Indian Politics in the Global Context: Promise and Implications." In: Sunetra Sen Narayan and Shalini Narayanan. 2016. Eds. *India Connected: Mapping the Impact of New Media*. (Pp. 79–105). Delhi: SAGE Publishing India.
- Salganik, Matthew. (2017). *Bit by bit*. Princeton: Princeton University Press. ISBN: 9781400888184.
- Schroeder, Ralph. 2016. Rethinking Digital Media and Political Change Convergence. *The International Journal of Research into Media Technologies*. <https://doi.org/10.1177/1354856516660666>.
- Sen Narayan, Sunetra, and Shalin Narayanan. 2016. Eds. *India Connected: Mapping the Impact of New Media*. Delhi: SAGE Publishing India.

- Shashank Bengali, Parth M.N. 2020. "TikTok Made Stars Out Of These Villagers In India. Then It Was Banned." *Los Angeles Times*. July 2, 2020.
- Simanowski, Roberto. 2018. *Stumme Medien*. Matthes & Seitz Berlin Verlag.
- Singer, Natasha. 2017. "How Google Took Over The Classroom." *The New York Times*. May 13, 2017.
- Sinha, S. 2021. More options for learning with Google workspace for education. Google [blog]. URL: <https://www.blog.google/outreachinitiatives/education/google-workspace-for-education>.
- Solon, Olivia. 2017. "'It's Digital Colonialism': How Facebook's Free Internet Service Has Failed Its Users." *The Guardian*. July 27, 2017.
- Sullivan, John L. 2013. "Uncovering the Data Panopticon: The Urgent Need for Critical Scholarship in an Era of Corporate and Government Surveillance." *The Political Economy of Communication* 1 (2). URL: <http://www.polecom.org/index.php/polecom/article/view/23/192>.
- Swedish Municipalities and Regions [Sveriges Kommuner och Regioner]. 2019. "Frågor Och Svar Dataskyddsförordningen För Skolan." January 1, 2019. URL: <https://skr.se/skolakulturfritid/forskolagrundochgymnasieskola/digitaliseringskola/dataskyddsfordataskyddsfor/fragorochsvardataskyddsforderordningenforskolan.15637.html#5.c697d52160463c55d043de1>.
- Telecom Regulatory Authority of India. 2016. "Prohibition of Discriminatory Tariffs for Data Services Regulation, 2016." February 8, 2016. URL: https://trafai.gov.in/sites/default/files/Regulation_Data_Service.pdf.
- Travizano, Mat. 2018. "The Tech Giants Get Rich Using Your Data. What Do You Get In Return?" *Entrepreneur*. September 28, 2018.
- Van Looy, Jan and Jan Baetens. (2003) *Close Reading New Media: Analyzing Electronic Literature*. Leuven: Leuven University Press.
- Vaidhyanathan, S. 2011. *The Googlization of everything: (and why we should worry)*. Berkeley: University of California Press.
- Wittel, Andreas. 2013. "Counter-Commodification: The Economy of Contribution in the Digital Commons." *Culture and Organization* 19 (4): 314–31.
- Yadav, Jyoti. 2020. "'We're Devastated, My Wives Cried' – TikTok Stars In Maharashtra Village Crushed By App Ban." *The Print*. June 30, 2020.
- Zuboff, Shoshana. 2019. *The Age of Surveillance Capitalism*. London: Profile Books.