Black Box versus Black Bloc

Renée Ridgway

rr.mpp@cbs.dk / rridgway@cc.au.dk

Abstract

With around 5.5 billion requests per day, Google is the most used search engine worldwide. Google Search identifies users online by collecting personal data—including an IP address, yet when using the Tor browser, a users' IP address remains obscured. *Black Box versus Black Bloc* employs Alexander Galloway's eponymous essay to structure the effects of Google Search (*The Personalised Subject*) compared to that of the Tor Browser (*The Anonymous User)*. Departing from the "data subject," I adopt the internet protocol (IP) address as an organisational hinge to show the effects of search on (us)ers —"subjectivities of search" and "agencies of anonymity," organised into 'collaborative collectives' according to degrees of human-algorithmic interaction. The key difference is that I choose to be in the "anonymous Tor collective," trusting my privacy to unknown human actors instead of putting trust in Google that assigns me to particular groups through their non-transparent process of collaborative filtering, without human agency.

Keywords

Search engines, Google, Tor, personalization, anonymity, black box, black bloc, subjectivity, agency.

DOI

10.69564/ISEA2023-80-full-Ridgway-Black-Box-vs-Black-Bloc

Introduction

"Many people I have talked to have mentioned that they are careful about what they type into search engines because they know it's being recorded and that limits the boundaries of their intellectual exploration."[1]

Since the rise of information technologies during the past 50 years, searching online has become one of the most popular human activities. With around 5.5 billion requests per day, Google is the most used search engine worldwide. Whereas ubiquitous computing described how electronic devices are interconnected, thereby making the communication of data pervasive,[2] the sociotechnical organization of "ubiquitous googling"[3] is now a daily habit where "users" searches produce data that make users findable, even as they wander.[4] With their IP (Internet Protocol) address collected as well as keyword searches and search histories, the past 20 years users frequently employed Google for information, medical advice or even research, thereby creating vast amounts of data. This "database of intentions" is now "a massive clickstream database of desires, needs, wants, and preferences that can be discovered, subpoenaed, archived, tracked, and exploited for all sorts of ends."[5] One of the ends is personalisation as currency, where users pay with data and what they receive are the currency of the web—customised URLs, based on their searching habits (browsers, location, histories).[6]

Besides data collection, the incorporation of user interaction—keyword search queries, impressions and clicking on links—is tied to an economic logic, advertisement, which facilitates ranking and recommendation on the part of the platform that intervenes.[7] This type of platform capitalism[8] is disrupting entrenched business models by highlighting as well as hiding—downplaying the labour of users and free data as platforms promote the horizontality of their services—yet they are not flat. Google Search "is a personal information economy where the standard exchange is service for profile"[9] part of the capitalistic "service/dataprofile/ advertising complex."[10] Thus, over time, Google transferred itself into an advertising company, producing not just search results, but capitalising on "informational rationality of generating value from advertising and audience labour."[11]

Through human-computer interaction with their ubiquitous googling, human bodies and their cognition, affect and interests have become valuable resources as data-subjects. With the "extraction activities" of user data by Google, a new asset class was created, or "surveillance assets"—providing a genuine market exchange.[12] Yet this data shapes users reciprocally through human-computer interaction. This results in fragmentary user subjectivity in deterritorialized spaces and it is the transformations of search subjectivities, where "bodies are mostly addressed at the level of affect and cognition"[13] that is cause for concern. The thoughts and values of users that are inscribed in queries are transferred into predictions, which subsequently produce not only products for corporations but incites changes in users' search behaviour. Thus, the habit of search by users produces enormous amounts of data, generating profits for Google but also facilitating the recursive feedback loop that organises (us)ers.[14]

However, there are ways to circumvent personalization and to reimagine search. Building upon the notion of "cyberspace privacy" that applied encryption technologies during the 1990s,[15] at the beginning of the last decade the 'privacy turn' took effect. The Nymwars (2010-2014) debated pseudonymity (the ability to have hidden identities when online) and the Snowden revelations (2013) exposed Five Eyes surveillance on citizens and corporate collusion. This resulted in an increase in usage of privacy technologies such as Tor (The Onion Router), an anonymity p2p browser that is a means to search online without divulging a user's IP address. Although controversial, there are many situations and "rationales for anonymity"[16] which are dependent on the context and situation, offline as well as when searching online.

This paper draws on my small data sets from an "experiment in living"—searching as a personalised subject with Google and an anonymous user with Tor. Departing from the data subject, I use the IP address as an organisation hinge to demonstrate the effects on (us)ers through a discourse analysis and a diagram. I combine these effects with Alexander R. Galloway's *Black Box, Black Bloc*,[17] which provides a conceptual (and technological) framework to synthesise the results from these two search methods. Derived from the effects, I then explain how each 'collaborative collective', *Subjectivities of Search* (Google) or *Agencies of Anonymity* (Tor) differs, based on degrees of human and non-human interaction.

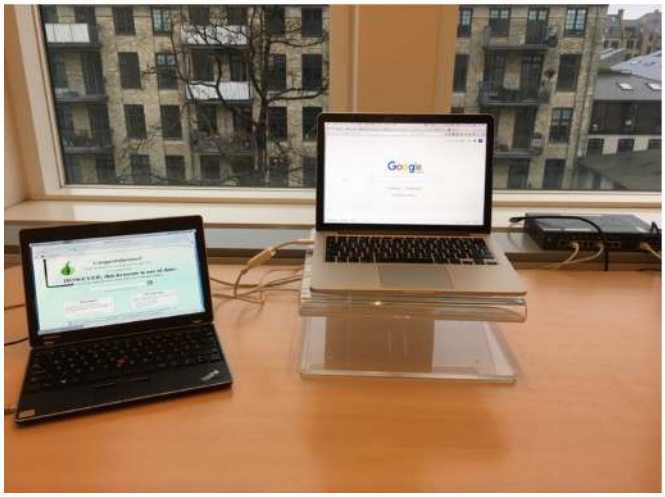

Figure 1: Experiment in Living: Google vs Tor

Experiment in Living: Google vs Tor

In order to discover how Google search organises (us)ers, I designed an "experiment in living"[18] and collected data on myself in my office. (Figure 1) This small study facilitated my understanding of the behind-the-scenes constellations of agents (protocols, algorithms and myself) that determined my search results. The research was conducted on two computers: one using Google search in a Firebox browser on a completely 'personalized' Mac (signed into a Gmail account, no ad blocking plug-ins, no incognito, etc.). With personalisation, Google customizes its algorithms in regard to IP address, keywords queried, search history and browsing habits to offer relevance and recommendations. The other computer is a Lenovo PC with a Debian operating system running the Tor browser that ostensible offers anonymity by hiding the IP address.

I used a set of keywords selected from texts I was reading at the time (2016) and I call this dataset *Re:search: Terms of Art*: Accelerationism, Aesthetic Turn, Anthropocene, Artistic Research, Contemporaneity, Creative Industries, Cultural Entrepreneurship, New Aesthetic, Object Oriented Ontology, Performativity, Post Digital, Post Humanism, Post Internet, Post Media, Transmedia. I gathered the data manually (I did not programme it to scrape the data) and saved the entire web page of the 1st page of results, along with the 10th, 20th, 30th, 40th and 50th etc. pages for the data set. This empirical 'experiment in living' in my office enabled me to capture two forms of address when searching online, one as a personalised subject with my IP address recognized by Google contrasted by being anonymous online with Tor, where my IP address is hidden.

Black Box, Black Bloc

One of the ways the protocological 'determines control after decentralisation' is through the configuration of the relationship between TCP/IP and DNS (Domain Name Server), as they are "political technologies." [19] TCP/IP is now the standard internet protocol suite and DNS, which runs parallel to HTPP in the application layer (7th), is responsible for translating the domain names into numerical IP addresses in order to identify devices and locate them within the network protocols. Google Search facilitates not only communication between parties to deliver search results (and advertisements), but the identification of 'subjects' and data collection, including the IP address. Conversely, with the Tor browser, the IP address is part of the protocol that facilitates the transport of data but the IP address is not revealed because of layers of encryption within the Tor p2p network.

By applying the IP address as an organisational hinge, I show the effects of search engines on (us)ers, drawing on my results as a "personalised subject" and as an "anonymous user." With a 'personalised subject', the black box and the Intellectual Property (IP) of Google's proprietary search algorithm is a form of "[in]visibility management."[20] situated within the "media arcane."[21] This blackness of the black box is also found in the Black Bloc that is analogous to tactics of obfuscation,[22] such as the Tor Browser, which, by obscuring the user's IP address, facilitates an anonymous user. I apply Alexander R. Galloway's Black Box, Black Bloc as a conceptual (and technological) framework to synthesise results from my two methods of search: "The black box: an opaque technological device for which only the inputs and outputs are known. The black bloc: a tactic of anonymization and massification often associated with the direct-action wingof the left. Somehow these two things come together near the end of the twentieth century. Is there a reason for this?"[23]

In the following I show the effects of these two methods of searching through a progression of human/algorithmic interaction. The structure of both these effects begins with search algorithms interacting with myself as a researcher collecting data online and as a data subject, who is protected by law. Since May 25, 2018 the GDPR (General Data Privacy Regulation) has been implemented in Europe, which regulates the collating,

processing, storage and transmission of personal data of EU citizens, or data subjects.[24] According to Article 4, the "data subject" is an end user whose personal data can be collected through 'direct identification' with an IP address. It is the recognition of citizens as 'data subjects' by their IP address that facilitates certain effects and the organization of those searching online—through degrees of personalisation (black box), or not, with degrees of anonymity (black bloc).

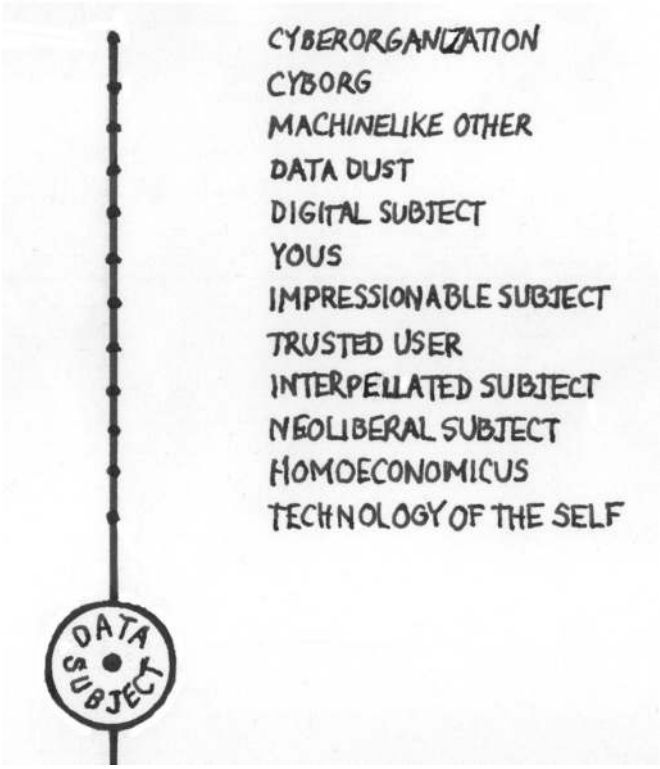

Figure 2: Subjectivities of Search

Black Box (Subjectivities of Search)(Figure 2)

During my experiment in living, I interacted with Google Search algorithms and used tools, such as my computer, as memory extensions or *hupomnemata,* to 'note down' and collect data on myself—keywords and search results. This Technology of the Self can be used as an instrument to analyse the relationship between the subject and truth, where the 'personalised subject' explores power constructs—how the subject constituted itself in one form or another, where "power is games of strategy."[25] As my search histories are constantly collected by Google Search, the 'personalised subject' is not a substance but a form, which is "not primarily or always identical to itself" as it is changes in different contexts and situations. Through diverse practices such as online interaction with search algorithms as "truth games," this modern day "technology of the self" transforms me as a (data) subject. Personalised subjects google themselves at some point, either to measure their attention economy—where everything is based on visibility—or to see what has been written or published about them by search results and that they are indexed.[26] It has become the meter to measure success. Appearing higher in Google's ranking, adding to one's visibility, is a particular kind of attention seeking that embodies Foucault's figure of the "Homoeconomicus," or economical man.[27]

Foucault was interested in the subject and more specifically, "the way a human being turns himself into a subject" and part of his scholarship looks at the history of discipline and what he came to term "biopolitics." "Foucault uses the term 'biopolitics' in order to elucidate how political power is carried out on every aspect of human life, making individuals and the Homoeconomicus someone who is eminently governable."[28] Although the Homoeconomicus is often considered a rational agent in pursuit of self-interest, these subjectivity-defined ends are part of an economic civil society that operates through production and exchange, which is part of the technology of liberal governmentality. Calculated practices (such as Google Search), permit individuals to govern themselves, which epitomises the biopolitical and lies at the core of neoliberalism. Google search facilitates online tracking and (self) surveillance, simultaneously optimising searching subjects who are also "[n]eoliberal subjects—small sovereigns—are always searching, rarely finding."[29] Through this interaction, the subject is both recognised, and subject to, the law.

In the early days of neoliberal capitalist ideology, before it was defined as such, Louis Althusser articulated forms of address through the framework of ideology, which he deemed "interpellation." With the constitutive process of interpellation, this ideology is recognised by the individual's acknowledgement of becoming a subject that complicates their domination and subjugation. The classic example is that of Althusser's policeman who shouts at a passer-by "hey, you there!" in public where the individual then responds by turning around. "[B]y this mere one-hundred-and-eighty-degree physical conversion, he [sic] becomes a *subject*."[30] Previously it was the police who asked the question: "Hey you there?" Nowadays 'personalised subjects' enhance the power structures of Google by recognising themselves as subjects when searching online, who are interpellated as "subjects" by automatically acknowledging the ideology of Google Search by deciding to use it. By clicking on links mostly found on the first page of Google, Brin and Page's "Trusted User" interacted with the search engine and reinforced this 'preferential attachment."[31] The Trusted User thereby actuates the

‘relevance’ and ‘quality’ of the search results by supplying feedback and data to Google, which it incorporates into subsequent search results.

In this orchestration of individuals and algorithmic actors on the stage of the internet, the efficacy of ‘online display advertising’ comprises not only the agency of human actors but algorithmic ones. By interacting with content on various websites, including Google Ads, visits are recorded by tracking cookies that are instilled by another actor, the ‘ad server’ and the ‘individuated subject’ produces a shadow. In the flow and ‘circulation of agency’ through its hyperlink journeys and its search queries…

"*The impressionable subject is produced as what is being visited and what is being searched*."[32] Searching subjects provide data to Google, facilitating the tracking of "YOUs" that "resonates strongly with Louis Althusser’s theorization of ideology," which "represents the imaginary relationship of individuals to their real conditions of existence."[33] Whether there is "caring of the self"[34] or caring of the network (the other YOUs), with the "interpellated subject’s" interaction with platforms such as Google Search, it becomes an effect of algorithmic ideology.[35] Sorted together with others like them, versions of multiple data selves are fed back through never-ending and recursive algorithmic loops. Comprised of a complexity of user subjectivities, the YOU addressed by Google search is, crucially, both singular and plural yet "[i]n its plural mode, though, it still addresses individuals as individuals,"[36] reflecting what has come to be called the Digital Subject.

The Digital Subject is an abstracted persona created from various data, records and archives, aggregated together to form what comes ‘after the subject, requiring new ways to understand how it connects to the subjectivities of living persons, something that is mapped onto living persons. With profiles in constant flux, temporalities and degrees of correlation supposedly enable better personalisation and "[i]t is also through the distance that digital subjects become more or less personalised or multiple—put together and disaggregated." [37] This ‘real-time’ collation of data on the "data subject" a.k.a. a Trusted User of Google Search, creates algorithmically produced entities of ‘Data Dust’ as an object of knowledge, which is comprised of dividuals [38] data shadows[39] data doubles[40] and data derivatives. [41] These simulacra are not representative of real ‘individuals’. Instead, they are encompassing elements, bits, points—"the fragments of registered behaviour, which are extracted from the flow of data for specific purposes."[42] These entities of Data Dust find others like themselves not in the "meat space" apartments of urban cities, or in towns scattered across flatlands, mountains andvalleys, but in worldwide data centres.

These numerous entities of the subject—*Subjectivities of Search*—are constructed by the very data that ‘personalised subjects’ give away when habitually searching online. Nowadays the subject ‘is potentially reduced to the pure $ (the divided subject)’ as a ‘Machinelike Other’. [43] Moreover, the construction of the ‘digital subject’ stems from the continuous production of inscribed personal data, resulting in ‘new forms of subject construction that arise out of computational procedures and are employed by various forms of power to distinguish, map, and capture not only subjectivities, but also non-humans and physical things that inhabit the world’. [44] Engaging with algorithms of Google Search, this hybrid form is Haraway’s cyborg—a site of contestation, challenging any traditional demarcation line between the human and the machine and instead defers to a space of patterning through the very technologies that comprise the database. Expressed otherwise, with the reconfiguration of subjectivities through technics and distributed cognition, ‘human bodies as cyborgs—as human machine systems—are in turn systematically combined into modes of “Cyberorganization”’. [45] As with the cyborg, Cyborganization is not an extension of the human agent but perhaps rather ‘the agent is an extension of the machine’ and ‘remains forever unfinished’, simultaneously controlling the flow of information back to searching subjects. [46]

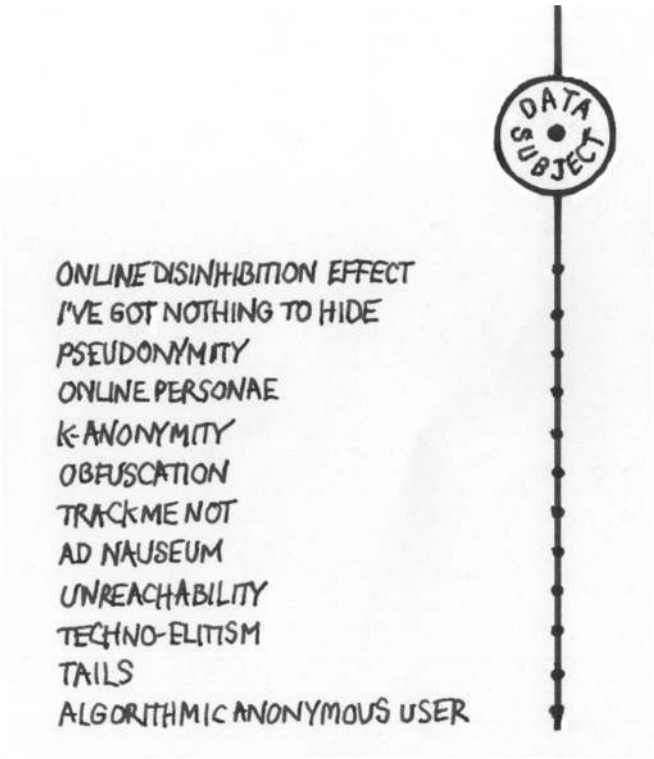

Figure 3: Agencies of Anonymity

Black Bloc (Agencies of Anonymity)

In the preceding section, I explained the effects, *Subjectivities of Search*, determined by the Black Box (Google Search). I return now to the other half of Blackness, the Black Bloc and its effects, based on my method of searching with the Tor browser (Figure 3).

The 'Online Disinhibition Effect' argues that online behaviour differs from 'real' world behaviour, emphasising the notion of invisibility because when people communicate with each other online they mostly do so in written form, as they do not see each other and thus are more apt to express themselves without inhibition. [47] In regard to the Snowden revelations, when asked whether spying on citizens is justified and whether citizens should be willing to exchange privacy and anonymity for increased security, the predominant rationalisation is that state surveillance is positive as it protects people from terrorism, often ending with 'I've Got Nothing To Hide'. However, people often feel immune to surveillance because they haven't committed a crime, yet '[a]ccountability is commonly raised as one of the reasons behind which people should provide identifiable information in online settings. When people prefer not to share their names, they're assumed to have something to hide'. [48]

In the early days of the web, '[t]he ability to participate anonymously or, as was and remains far more common, pseudonymously was an integral part of why Barlow and other net utopians saw the Internet as valuable'. [49] In the 1990s users had 'monikers' when they signed into chatrooms, later on they created email addresses for each different service they signed up for. Besides 'traffic analysis' and 'mixed networks'—the basis for Tor encryption— Chaum's other contribution to knowledge included 'digital pseudonyms', which is 'a public key used to verify signatures made by the anonymous holder of the corresponding private key'. [50] Weisner, described 'digital pseudonyms' as a means to insure privacy within networked societies. [51] Instances of Pseudonymity do not mean that one is completely anonymous, rather various pseudonyms can be linked together to form either an 'online identity' or Online Persona, which 'had come alive in a new social practice: the virtual world as context for explorations of identity'. [52] One reason to build these constructed online personas is that they 'also offer sites of reinvention, liberation, and play. Fake accounts and performed identities testify to that'. [53]

Persona building goes hand in hand with crawling the Dark Net in that it is replete with pseudonyms and false identities. In attempts to reach 'total anonymous freedom' Dark Web Social Net (DWSN) members 'customise their aliases, avatars, pseudonyms through widgets and in such a way that '[o]ne does not use a fake account every time; one builds a *persona*'. [54] When all of these pseudonyms are collated by malevolent actors to construct personas, together they can form an online profile. However, there are tactics to prevent this from happening. *K-anonymity*: *A model for protecting privacy* would alter released information based on scaling, where the greater number of candidates, the 'more ambiguous the linking, and therefore the more anonymous the data'. [55] Analogous to the increased strength of anonymity with a larger amount of Tor users, the efficacy of 'scaling' tactics with *K-anonymity* are nowadays limited due to fact that the storage of data continues to become easier and cheaper as computational power increases and companies can examine this information in 'real time'.

In regard to these problems, Obfuscation is necessary in an era of online tracking and its use-value is in 'mitigating and defeating present-day digital surveillance'. [56] Applying tactics of secrecy and deception to combat asymmetrical relationships of power, the guide shows various methods of resistance that, while they might be considered 'weapons of the weak', afford some amount of autonomy for the user. Moreover, these tactics prevent various shields of recognisability—how signals or information could be interpreted, transmitted or shared by enemy parties. With personalisation, the IP address plays a crucial role in the identifiability of the user along with the ever-

increasing amount of data collected and shared between search engines and third parties. As a reaction to the public realisation that search companies (notably Google) were logging, storing and analysing the search query logs of individuals, 'TrackMeNot' (TMN) is 'designed to achieve privacy in web search by obfuscating users' queries within a stream of programmatically generated decoys'. [57] Another 'tactical media', AdNauseum is a browser extension that floods Google Search with false queries, clicks and likes *all* ads, concomitantly visualizing the ads. [58]

Although obscuration offers many shades of privacy, a 'true inner self' can only emerge in anonymity. [59] The shift from the ability to carry out actions 'namelessly' in offline space 'is not as the end in itself of anonymity', rather it is about how users can conduct themselves anonymously online, whether a person is identifiable (or not) as themselves and if they are untrackable. This 'Unreachability' is where absence can be used for positive expression in the complex and dynamic computer-oriented society. Already in 1999 Nissenbaum presciently predicted the era of 'surveillance capitalism' where every atom of data is collected, kept and analysed: 'Information technology has made it possible to track people in historically unprecedented ways. We are targets of surveillance at just about every turn of our lives'. [60]

With *Agencies of Anonymity*, users can consciously protect themselves against the 24/7 tracking of surveillance capitalism through tactics of obscuration yet this 'unreachability' reflects an acquired knowledge —having the 'tech savvy' to use Tor. Spurred by agencies of 'control' over one's data, this Techno-Elitism is a type of self-determination[61]—knowing how to obtain anonymity and remain hidden from search engines and governmental agencies. Furthermore, there are those 'techno-elitists' who do not wish to be indexed by Google and desire to remain 'unreachable' to search engines, or delete their information after searching with Tor. TAILS is an operating system that has Tor already configured, which, installed on a USB stick, boots the computer and everything is deleted upon ejection.[62] Or, if one desires to be undetected and shop, the tactical media cum art project *Random Darknet Shopper (2014-ongoing)* by! Mediagruppe Bitnik is a programmed autonomous bot that searches the Dark Net and carries out purchases, completely anonymously, albeit through code.[63] However, this Algorithmic Anonymous User raises an important question regarding the accountability of actions by non-human actors: can one prosecute and punish an algorithm that commits a crime, in this case purchasing illegal substances and sending them to the St Gallen Kunst Halle by post for an art installation?

Collaborative Collectives: Agencies of Anonymityvs. Subjectivities of Search

Returning now to my results from comparative searching using Google's personalisation and Tor's anonymity, I learned that Tor delivers 'Google-like' results with its default search engine, only without personalisation and targeted ads because there is no captured locative data, search history or IP address. However, if I assume that both is the case—on the one hand, I am assigned as a Tor user and on the other that Google assigns me to groups of people like me on its databases (an assumption I cannot fully prove with my experiment but is the most likely scenario to explain its outcomes)—the original framing of my experiment has to be specified. Instead of a personalised search as opposed to an anonymised search, I would have, in fact, conducted a Google search that is a collective-of-users-like-me versus a collective-of-all-Tor-users. At stake, therefore, are two collectives that take different *forms*.

In the collective-of-users-like-me it is Google's algorithms which construct the categories I am part of and assign me to this or that collective (e.g., collaborative filtering). I have no access, no knowledge and no agency in regard to the collectives which I am made part of via Google. The forces (identification markers: IP address, search histories, cookies, supercookies and locative data) that sort me into a collective and the collectives that I am organised into—the categories that Google sets up and assigns me to, are not transparent to me. Moreover, Google collects my individual search activities and, in future scenarios, will probably state that they 'personalise' search even further based on data collated in the past and present.

Tor's collective, on the other hand, is both an anonymity network *and* a browser—Tor is mostly Firefox code (95%) that incorporates patches to Firefox ESR (Extended Support Release). The Tor collective is at least partially known to me as university labs worldwide run the major nodes but I do not know who is running the relays (it is an anonymised network). I can, however, look at the 'exit address' list, which is constantly updated and shows the IP address, though I cannot identify the users.[64] By joining the Tor collective I decided to trust the exit node operators, also in regard to my 'expectation of privacy'. The key difference is that

whereas Google organises me into particular collectives through their non-transparent process of collaborative filtering, I decided to be organised into the 'anonymousTor collective'. (Figure 4)

Figure 4: Agencies of Anonymity vs. Subjectivities of Search

Both search collectives, the one determined by Google's algorithms as well as the one created by the choice to use Tor, add to specific filter bubbles. The filter bubbles are, however, structurally different: in the case of the bubble produced by Google's algorithms, Google collects the data of its users and incorporates user feedback into subsequent search results. When I search for different things, I am merged into different clusters with *other* people 'like me' or 'YOUs'. I would then add to the feedback loop by continuously adding to my own personalisation by clicking on the links that are delivered to me as results. I do not have access to the Google collective itself—I am constantly switched into a different cluster by an algorithmically organised process that I have no control over and cannot adjust. There are also constant updates and tweaking of signals being carried out on the algorithm. Therefore, I propose that various degrees of Google Search's personalisation organise the corporal 'data subject' into effects: *Subjectivities of Search.* With the *Black Box*, as Google's personalisation increases so does the amount of computational agency, at the same time the degree of anonymity (privacy) decreases.

The filter bubble of the Tor users, on the other hand, is one where I stay in the same group that shares the same filte—no matter how much I change my search behaviours (what I click on or not). As a Tor user, the variable is what Tor uses as their default search engine (Startpage, Disconnect Search or presently DuckDuckGo) and if this default (still) delivers Google Search results without locative data. Therefore, the results of my small data experiment postulate that the user is assigned the category of 'Tor user', which can be seen from outside the Tor network. When I use Tor I am part of a p2p anonymity network, which increases in strength the more users use it. Unlike Google Search, privacy-enhancing technologies and diverse settings

enable the user to organise themselves into effects: *Agencies of Anonymity*. With the *Black Bloc*, as the amount of anonymity (privacy) increases with Tor so does human agency, at the same time the degree of personalisation decreases. If I compare these two search processes, with the *individualisation* of the pseudo-autonomous objects of Google's personalisation, my 'data dust' is atomized and fractured—as a 'digital subject' I have no agency to decide where I am assigned. However, to partake anonymously in a p2p-collective *individuates* me more than personalisation does. Bernard Stiegler's entire pharmacology of care revolves around this new ecology, which can be understood to be threefold, as a 're-articulation of psychic, collective and technical *individuation*'. [65] At stake is an *individuation* in the sense of Stiegler's reading of Simondon—an *individuation* that is marked by being collective and psychic alike, where the genesis of how an object comes to exist is through operations of *individuation,* or 'ontogenesis' and a living being exists in a state of becoming between individuations, never in isolation but in collective, social as well as psychological constellations. The Tor browser (p2p network) embodies this individuation of collective singularities, which are dependent on the other. 'After all, an individual exists and is only capable of individuating as a result of the relations it establishes with others and that others establish with it.' [66] Phrased otherwise, the possibility of choosing the *individuating* Tor collective over the *individualisation* of Google Search might be a modest resolution to the problem of 'how one would define a singularity that could be a collective singularity'. [67]

The experience of setting up an 'experiment in living' has opened up a *view* on how Google Search works and my exploration of using Tor reimagined what search could look like. Without having to become a 'personalised subject', Tor offered me 'relevant' search results as an 'anonymous user'. With the Tor Browser I am not 'commanded' by 'prescriptive' technologies [68] as I am with Google Search, instead I chose which collective I wished to be part of, in this case Tor. The effects of the Black Bloc (*Agencies of Anonymity*) enabled me to intervene and this type of searching facilitated degrees of anonymity, embodied by various levels of user agency. Aside from its other merits, Tor is also one, albeit not the only, strategy to challenge the protocols facilitating Google's 'surveillance capitalism'.

References

1 Laura Poitras *Citizen Four,* 2014, https://citizenfourfilm.com/

2 Mark Weiser, "The Computer for the 21st Century". *Scientific American* Special Issue on Communications, Computers, and Networks, September, New York, *Scientific American*, 1991.

3 Renée Ridgway, Re:search. Dissertation, 2021.

4 Wendy Hui Kyong Chun, *Habitual New Media: Updating to Remain the Same,* Cambridge, MIT Press, 2016, 77.

5 John Battelle, *The Search: How Google and Its Rivals Rewrote the Rules of Business and Transformed Our Culture,* New York Penguin, 2006, 6.

6 Renée Ridgway, "Personalisation as currency", *APRJA* (A Peer-Reviewed Journal About), 18 APRJA Volume 4, Issue 1, 2015, http://www.aprja.net/?p=2531.

7 Tarleton Gillespie, "Platforms Intervene", *Social Media + Society,* Thousand Oaks: Sage Publishers, 2015.

8 Nick Srnicek, *Platform Capitalism,* Cambridge, Polity Press, 2016.

9 Greg Elmer, *Profiling Machines: Mapping the Personal Information Economy,* Cambridge, MIT Press, 2003.

10 Geert Lovink, Nathaniel Tkacz, "MoneyLab: Sprouting New Digital-Economic Forms", In *Moneylab: An Intervention in Digital Economy,* Amsterdam, Institute of Networked Culture, 2015, 15

11 Dallas Smythe, "On the audience commodity and its work", in M. G. Durham, D. M. Kellner (eds) *Media and cultural studies,* Malden, MA, Blackwell 1981, 230–56

12 Shoshana Zuboff, "Big Other: surveillance capitalism and the prospects of an information civilization", *Journal of Information Technology,* 30, Thousand Oaks: Sage Publishers, 2015, 81

13 Armin Beverungen, Timon Beyes, Lisa Conrad, *Digital Media,* Thousand Oaks, Sage Publishers, 2019.

14 Renée Ridgway, Re:search. Dissertation, 2021.

15 David L. Chaum, "Untraceable Electronic Mail, Return addresses, and Digital Pseudonyms", Communications of the ACM, Volume 24, Number 2, February 1981.

16 Gary Marx, "What's in a Name? Some Reflections on the Sociology of Anonymity",*The Information Society*, 15:2, Milton Park, Taylor & Francis, 1999, 99- 112.

17 Alexander R. Galloway, "Black Box, Black Bloc." In: Benjamin Noys (ed.): *Communization and its Discontents. Contestation, Critique, and Contemporary Struggles,* Brooklyn, Minor Compositions/Autonomedia, 2011, 237–249.

18 Noortje Marres, "The Experiment in Living", In *InventiveMethods: The Happening of the Social*. Celia Lury, Nina Wakeford. Eds, Abingdon, Routledge, 2012.

19 Alexander R. Galloway, *Protocol: How Control Exists afterDecentralization,* Cambridge, MIT Press, 2004.

20 Mikkel Flyverbom, Paul Leonardi, Michael Stohl, Cynthia Stohl, "The Management of Visibilities in the Digital Age: Introduction", *International Journal of Communication*, Los Angeles, USC Annenberg Press, Vol. 10, 2016, 98–109.

21 Timon Beyes, Claus Pias, "The Media Arcane." *Grey Room* 75, Cambridge, MIT Press Journals, 2019, 84-107.

22 Finn Brunton, Helen Nissenbaum, *Obfuscation, A User's Guide for Privacy and Protest,* Cambridge, MIT Press, 2015.

23 Alexander R. Galloway "Black Box, Black Bloc.", 3

24 GDPR, General Data Protection Rights, https://gdpr-info.eu/art-4-gdpr/

25 Michel Foucault, *Ethics: Subjectivity and Truth, The Essential Works of Michel Foucault 1954-1984*.

26 Tarleton Gillespie, "2. Algorithm" In *Digital Keywords. A Vocabulary of Information Society and Culture*. Edited by: Benjamin Peters, Volume 8 in the series Princeton Studies in Culture and Technology, Princeton, Princeton University Press.

27 Michel Foucault, *Technologies of the Self,* Edited by Luther H. Martin, Huck Gutman, Amherst, University of Massachusetts Press, 1988, 16.

28 Philip Mirowski, *Never Let a Serious Crisis Go to Waste,* New York, Verso, 2013.

29 Wendy Hui Kyong Chun, *Habitual New Media: Updating to Remain the Same.*

30 Louise Althusser, "Ideology and Ideological State Apparatuses (Notes towards an Investigation)," In *Lenin and Philosophy and Other Essays*, translated by B. Brewster, London, Monthly Review Press, 1971, 174.

31 Sergei Brin, Larry Page. "*The Anatomy of a Large-Scale Hypertextual Web Search Engine",* Presented at Seventh International World-Wide Web Conference (WWW 1998), Brisbane, Australia, April p.14-18.

32 Lucas Introna, "The algorithmic choreography of the impressionable subject", In Seyfert, Robert and Roberge, Jonathan (Eds.), *Algorithmic Cultures: Essays on Meaning, Performance and New Technologies,* Abingdon-on-Thames, Routledge, 2016, 37

33 Wendy Hui Kyong Chun, *Habitual New Media: Updating to Remain the Same,* 121

34 Michel Foucault, *Ethics: Subjectivity and Truth, The Essential Works of Michel Foucault 1954-1984*.

35 Astrid Mager, "Algorithmic Ideology." *Information, Communication & Society*, 15:5, Milton Park, Routledge, 2012p. 769-787.

36 Wendy Hui Kyong Chun, *Habitual New Media: Updating to Remain the Same, 36, 64*

37 Olga Goriunova, "The Digital Subject: People as Data as Persons" *Theory, Culture and Society*. Vol. 36, No. 6, 01.11.2019, 125-145.
Thousand Oaks, Sage Publishers, 2019, 126

38 Gilles Deleuze, "Postscript on the Societies of Control", *October.* Vol. 59., Winter, 1992, 3-7, Cambridge, MIT Press, 1992, 5.

39 Nanna Thylstrup, "Archival Shadows in the Digital Age", *NordiskTidsskrift for Informations videnskab og Kulturformidling*, årg. 3, nr. 2/3, 2014.

40 Antoinette Rouvroy, "The end(s) of critique: Data behaviourism versus due process", In Hildebrandt, Mireille and De Vries, Katja (eds.) *Privacy, due process and the computational turn: the philosophy of law meets the philosophy of technology,* New York, Routledge Taylor, Francis Group, 2013.

41 Louise Amoore, "Data Derivatives: On the Emergence of a Security Risk Calculus for Our Times", *Theory, Culture & Society* 28(6), 24–43, Thousand Oaks, Sage Publishers, 2011, 126

42 Felix Stalder, "Between Democracy and Spectacle: The Front-End and the Back-End of the Social Web", In M. Mandiberg (ed.), *The Social Media Reader, New York, New York University Press, 2012,* 242-256.

43 Slavoj Zizek, *The Ticklish Subject: The Absent Centre of Political Ontology,* Brooklyn: Verso Books, 1999.

44 Friedrich A. Kittler, *Gramaphone, Film, Typewriter*. Stanford. Stanford University Press, 1999, 127.

45 Martin Parker, "Manufacturing Bodies: Flesh, Organization, Cyborgs". In Hassard, J., Holliday, R., Willmott, H. (Eds) *Body and Organization,* London, SAGE Publications 2000,73, 71-86.

46 Martin Parker, Robert Cooper, "Cyborganization: Cinema as Nervous System", In *For Robert Cooper: Collected Work,* Edited by Gibson Burrell and Martin Parker, p.236-252, New York: Routledge, 2016, 243.

47 John Suler, "The Online Disinhibition Effect". *Contemporary Media Forum International Journal of Applied Psychoanalytic Studies*, Vol. 2, No. 2., Jacksonville, N.C., Whurr Publishers Ltd., 2005.

48 Danah Boyd, "The Politics of 'Real Names: Power, Context, and Control in Networked Publics", *Communications of the ACM* 55(8): 29-31, 2012, 30.

49 Lisa Nakamura, "Afterword: Blaming, Shaming and the Feminization of Social", Shoshana Magnet and Rachel Dubrofsky (eds). *Media Feminist Surveillance Studies,* Chapel Hill, Duke University Press, 2014.

50 David L. Chaum, "Untraceable Electronic Mail, Return addresses, and Digital Pseudonyms", 1

51 Mark Weiser, "The Computer for the 21st Century", *Scientific American* Special Issue on Communications, Computers, and Networks, September, New York, *Scientific American*, 1991.

52 Sherry Turkle, *The Second Self,* Cambridge Mass, MIT Press, 2005, 288

53 Olga Goriunova, "The Digital Subject: People as Data as Persons" *Theory, Culture and Society*. Vol. 36, No. 6, 01.11.2019, Thousand Oaks: Sage Publishers, 2019, 125-145, 127.

54 Robert W. Gehl, "Power/freedom on the dark web: A digital ethnography of the Dark Web Social Network", Republished 2016, *New Media & Society*, Volume 18(7), 1219-1235, Thousand Oaks: Sage Publishers, 2014, 1226.

55 Lantaya Sweeney, "K-anonymity: a model for protecting privacy". *International Journal on Uncertainty, Fuzziness and Knowledge-based Systems*, 10. 2002, 557-570, Singapore, World Scientific Publishing Co Pte Ltd, 2002.

56 Finn Brunton, and Helen Nissenbaum, *Obfuscation. A User's Guide for Privacy and Protest,* Cambridge, MIT Press, 2015, 55

57 Helen Nissenbaum, Daniel C. Howe, "TrackMeNot: Resisting Surveillance in Web Search". In Kerr,I., Lucock, C. and Steeves,C. (Eds), *'Lessons from the Identity Trail: Anonymity, Privacy, and Identity in a Networked Society,* Oxford, Oxford University Press, 2009, 417.

58 Helen Nissenbaum, Daniel C. Howe, Mushon Zer-Aviv., *Ad Nauseum,* 2014, Available at: https://adnauseam.io

59 Daniel C. Howe, Helen Nissenbaum, "Engineering Privacy and Protest: A Case Study of AdNauseum". Proceedings of the 3rd International Workshop on Privacy Engineering, Volume 1873, 57-64, 2017, 57.

60 Helen Nissenbaum, "The Meaning of Anonymity in an Information Age", In Spinello, Richard A. and Tavani, Herman T. (eds.), *The Information Society*. 15:141-144n Milton Park: Taylor & Francis, 1999, 141

61 Robert W. Gehl, "Power/freedom on the dark web: A digitalethnography of the Dark Web Social Network".

62 TAILS, The Amnesiac Incognito Live System, https://tails.boum.org/

63 Random Darknet Shopper 2016, MediabitnikGruppe: https://wwwwwwwwwwwwwwwwwwwww.bitnik.org/r/

64 Tor Project: https://check.torproject.org/exit-addresses

65 Eric Hörl, *General Ecology: The New Ecological Paradigm,* London, New York, Bloomsbury Academic, 2017, 35.

66 Bernhard Stiegler, *To Love, To Love Me, To Love Us: From September 11 to April 21,* Stanford: Stanford University Press, 2009, 77.

67 Maurizio Lazzaroto, "Conversation with Maurizio Lazza-roto". Public Editing Session #3, June 23, 2010, from 'Exhausting Immaterial Labour in Performance'; joint issue of *Le Journal des Laboratoires and TkH Journal for Performing Arts Theory* (no. 17), October 2010, 14.

68 Ursula Franklin, "The Real World of Technology". Massey Lectures, 1989.