



Publisher: IISI - International Institute for Socio-Informatics

ISSN 1861-4280

# international reports **on** socio-informatics

Vol. 17, Iss. 1  
2020

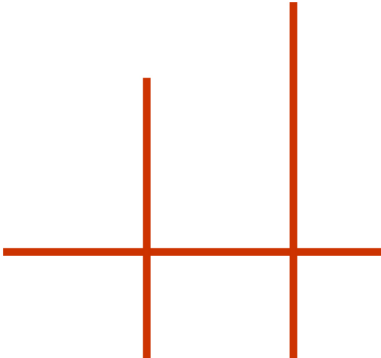
*Restraining Surveillance Capitalism:  
Alternative Designs for Social Media and  
Cloud Computing Platforms*

## **Guest Editors:**

Marvin Landwehr  
Alan Borning  
Volker Wulf

## **Editors:**

Volkmar Pipek  
Markus Rohde



*The 'international reports on socio-informatics' are an online report series of the International Institute for Socio-Informatics, Bonn, Germany. They aim to contribute to current research discourses in the fields of 'Human-Computer-Interaction' and 'Computers and Society'. The 'international reports on socio-informatics' appear at least two times per year and are exclusively published on the website of the IISI.*

## **Impressum**

IISI - International Institute for Socio-Informatics  
Stiftsgasse 25  
53111 Bonn  
Germany

fon: +49 228 6910-43

mail: [iisi@iisi.de](mailto:iisi@iisi.de)

web: <http://www.iisi.de>

# Table of contents

1	Introduction .....	5
2	Developments in the Computing Industry.....	8
	<b>2.1 A Takeover in IT .....</b>	<b>8</b>
	<b>2.2 Enabling Technologies.....</b>	<b>9</b>
	<b>2.3 Retaining the Benefits .....</b>	<b>11</b>
3	Problems for Democracy and Sustainability .....	11
	<b>3.1 The Root Causes.....</b>	<b>12</b>
	3.1.1 The Business Model      12	
	3.1.2 Surveillance Computing   13	
	<b>3.2 Sustainability Aspects.....</b>	<b>14</b>
	3.2.1 Consumerism and Excessive Consumption under Conditions of Relative Saturation   14	
	3.2.2 Consequences for Sustainability   15	
	<b>3.3 Political Aspects .....</b>	<b>16</b>
	3.3.1 Three Dimensions of Power 16	
	3.3.2 Free Speech and Participation Dimension   17	
	3.3.3 Privacy Dimension   19	
	3.3.4 The Dimension of Independence from Political Manipulation 20	
	<b>3.4 Surveillance Capitalism Undermining the Foundations of Society .....</b>	<b>21</b>
4	Possible Solutions .....	22
	<b>4.1 Regulation and Law .....</b>	<b>22</b>
	4.1.1 True Informed Consent   23	
	4.1.2 Adversarial Interoperability   25	
	4.1.3 Consequences for the Business Models   26	
	<b>4.2 Some Limitations of Regulation and Rejected Approaches.....</b>	<b>27</b>
	<b>4.3 Social Practice .....</b>	<b>29</b>
	4.3.1 Education   29	
	4.3.2 Resistance   30	
	<b>4.4 Technology.....</b>	<b>32</b>
	4.4.1 Useful Technologies and Practices   33	
	<b>4.5 Funding, Ownership, and Control .....</b>	<b>35</b>
	4.5.1 For-Profit Corporations   36	
	4.5.2 Public Funding and Public Control   36	
	4.5.3 NGOs and Cooperatives   37	
	4.5.4 No Funding or Minimal Funding   38	
	4.5.5 An Ecosystem Approach   38	
5	Conclusions.....	39
6	Acknowledgments .....	39
7	References .....	40

# Restraining Surveillance Capitalism: Alternative Designs for Social Media and Cloud Computing Platforms

Marvin Landwehr

Hochschule Bonn-Rhein-Sieg, Bonn, Germany

*marvin.landwehr@h-brs.de*

Alan Borning

Paul G. Allen School of Computer Science & Engineering,

University of Washington, Seattle, Washington, USA

*borning@cs.washington.edu*

Volker Wulf

Int. Institute for Socio-Informatics, Bonn, Germany,

and University of Siegen, Germany

*volker.wulf@iisi.de*

**Abstract.** A Over the past two decades, business models have emerged in the IT industries that have turned out to be highly profitable, but that, if left unchecked, will very likely destroy the foundations of liberal democracies and quality of life on this planet. The models involve customized advertising and behavior manipulation, powered by intensive gathering and cross-correlation of personal information. They allow a large portion of software, including web search, email, social media, and much more, to be provided “free” to the end users. Other parts of the IT infrastructure, such as e-commerce platforms, use a fee-for-service model but still are rooted in intensive gathering and cross-correlation of information. There are significant indirect costs of these business models, including loss of privacy, supporting surveillance by both the state and corporations, undermining the democratic process, other kinds of automated attempts of behavior manipulation, and excessive consumerism with its attendant environmental costs. Shoshana Zuboff conceptualizes them as “surveillance capitalism.” Drawing on many of Zuboff’s observations and extending her model, we characterize the different business models and suggest counter-strategies based on an analysis of their consequences. Our suggestions involve the co-development of regulation, technology and social practices. We argue that the advertisement- and surveillance-driven business models of the IT industry need to be strongly regulated to tackle the root of these problems and to create conditions for the emergence of alternatives; and then go on to suggest directions for such alternatives.

## 1 Introduction

In the IT industries, the expectations for profit have grown over the past two decades, similar to the banking industry until the financial crisis of 2008. In 2020, among the ten most valuable companies in the world (in terms of market capitalization), seven are IT companies: Microsoft, Apple, Amazon, Alphabet, Facebook, Alibaba, and Tencent. All of them share very similar business models (though Apple, differs with a focus on hardware), and were able to meet investors’ tremendous profit expectations. However, the implementation of the business models relies on extensive data gathering, and we will argue that the profitable monetization of such data comes at the expense of a devastating societal spillover. Based on the data they gather, these companies generate revenue by selling customized advertising or predicting and influencing their users’ behavior. User data becomes much more valuable (a) in contexts of past and planned purchases, (b) when data that corresponds to the same user can be connected from different contexts to generate a significantly more sophisticated user profile, (c) where profile data can be compared and correlated with similar profiles from the database, and (d) where data can serve as basis for attempted behavioral manipulation. Since it is their predictive and manipulative capital (Manokha, 2018), these big IT companies do not sell data directly, as that would undermine the basis of their business model. However, smaller companies exist whose business relies on expropriation of data (e.g., by employing trackers). They thus serve as additional data suppliers for the big IT companies. These small companies sell the data because it is most valuable at the point where it can be

correlated (see a–d above), which is at the big data silos. Thus, a data centralizing effect occurs. These data transfers are typically fully opaque to the end user. For the big IT companies, instead revenue is generated by predicting and influencing user behavior (Buettner, 2017).

Zuboff (2015, 2019) has named this business model “surveillance capitalism,” and we use this same term here as well. Her recent book makes clear that this is not simply an issue of surveillance and loss of privacy, but also an attempt at a radical and ominous automated manipulation of behavior that is undermining democracy, human dignity, and much more. One could read Zuboff’s perspective to imply that people can be arbitrarily manipulated — Lenhart and Owens (2020) summarize this as the myth that “social media is addictive and we are powerless to resist it.” Doctorow (2020) presents a similar critique that puts much more emphasis on individual choice and control. We could caricature extreme versions of these positions as (a) a behaviorist view that assumes people can be arbitrarily manipulated by targeted ads, carefully curated feeds of more and more provoking content, and so forth; and (b) a self-determination view — people have free will and they can simply decide for themselves whether or not to pay attention to the content.<sup>1</sup> Our own position is an interactional one: corporate manipulation of (for example) news feeds and content doesn’t rigidly determine particular responses by the users; but on the other hand, the design of the feed is not something that leaves people in total control. People’s social practices are shaped historically by the activities they conduct, as well as by artifacts and the way these are used. Information delivered by social media sites, as with any other IT system, affects human actors in their practice context. Thus, a certain news feed does not determine an overall behavioral reaction, but, depending on the context, reading those items it may make a particular action more likely. We can also make an analogy with a key element of the theoretical stance taken by value sensitive design (Friedman & Hendry, 2019; Friedman, Kahn, & Borning, 2006). (VSD is a theory and design methodology intended to better support important human values in the design of technology.) One of the key elements of VSD’s theory is an interactional stance, which posits that values are not indelibly inscribed into some given piece of technology, but on the other hand technological artifacts are not value neutral.

A compelling example of this in the context of surveillance capitalism is Facebook’s emotional manipulation study (Flick, 2016; Talbot, 2014), in which Facebook researchers ran an experiment on 689,003 users, testing whether they could manipulate their user’s moods by adjusting their news feeds to favor negative or positive content. There was a small but statistically significant effect. So Facebook’s users were not arbitrarily manipulated (with Group A having a joyous day and Group B a thoroughly miserable one, as a result of the changes to

---

1 These are indeed caricatures however — the actual views expressed by for example Zuboff and Doctorow are more nuanced.

their news feeds); but on the other hand, Facebook's technology was hardly value neutral, with their users free to attend to or ignore the positive or negative content. (Among other things, the users were unaware that they were being experimented upon.) This study was particularly controversial, since among other things there was no true informed consent from the users to participate in it — but we would point out that there is also no true informed consent to participate in the countless A/B studies that the corporations carry out for marketing rather than research purposes, or the emotional manipulation by advertising.

A consequence of taking an overly behaviorist stand that denies people their free will would fundamentally contradict democratic values. Proposed solutions that would lead to excessive censorship are therefore problematic in our opinion. Further, free will is meaningless without the ability to understand and foresee the consequences of one's own decisions. Applied to this problem, the attempted manipulation is a serious attack which one, nevertheless, is not powerless against. One can become aware of and break through these mechanisms. Therefore, a restrictive legal response to the practices of these companies is necessary, but only until people are empowered to notice the manipulation and understand the risk of using these free services and make an informed choice between them and possible alternatives. Practices for which this is not achievable should remain prohibited. That is the position we take and we will explore in the second half of this essay what that means for how to counter surveillance capitalism.

This heavy investment in advertising is characteristic of the state of capitalism in which economies of the global north tend to saturate. Growth is artificially stoked by ever more elaborate advertising methods that aim to increase consumption. Targeted advertising based on personal data profiles is considered to be currently the most effective of these methods. Even though surveillance capitalism has found a way to be highly profitable on the basis of services that are offered free of charge to the end user, free services are not its characterizing feature. Instead, data grabbing and monetizing it via attempted behavior manipulation are the characteristic properties of surveillance capitalism. The services can be expected to remain free only as long as the companies that offer them consider this as the most profitable way to gather relevant data. And the practices of data gathering are not limited to free services. Amazon is the archetype of a shopping platform that could have another source of income simply with brokerage fees, but that in fact makes significant profits by surveilling the purchasing behavior of buyers and the market situation of sellers, so the offers from third-party merchants can be replaced by Amazon's own if they sell well.

This orientation of IT companies not only produces centralized data silos, it nudges power relations toward centralization as well. Furthermore, it has resulted in the creation of technological infrastructures that have significantly shaped the software industry during the last two decades. To be able to amalgamate data taken from different devices and operating systems and process them centrally,

software and data architecture were needed that were later commercially offered as a service in the form of cloud computing. Applications provided in the cloud store the data in a centralized manner, typically on a server infrastructure of the service provider; they tend to expropriate data ownership. Moreover, the functionality is offered to all users in a rather standardized manner, and offers only limited opportunities for users to tailor or individualize them. To partly compensate for this limitation, the leading surveillance capitalist companies have developed Machine Learning technologies to automatically adapt the functionality (e.g., filtering or sorting algorithms in social media platforms).

In this sense, Machine Learning is a data centric approach to individualization by an automated approach that is based on large volumes of standardized data.

However, we argue that the economic successes of the surveillance capitalism business models have radiated throughout the computing industry, and are in the process of moving it in a socially problematic direction. In particular, we describe in Section 3 how they endanger liberal democracies, provide additional tools for surveillance and control to autocratic government, and threaten the quality of life on this planet. We then situate the role of these business models in the conflict between growth imperatives and sustainability. Next, we differentiate three dimensions in which these services undermine the sovereignty of humans and therefore conflict with democratic values.

Section 4 is our response to this problem statement. It elaborates, what was summarized in our policy brief for the G20 insights forum (Bennett, Borning, Landwehr, Stockmann & Wulf, 2020). We suggest a co-development of regulation, technology and social practice in order to undermine the currently dominant IT business model that is at the heart of surveillance capitalism, and to foster the creation of alternative services that are more aligned with democracy and quality of life. We describe how the measures in these three areas interact with each other and show where they counteract the problem dimensions that we have identified. Finally, we argue for an ecosystem approach as a counter narrative to surveillance capitalism and discuss the crucial role of ownership structures for these IT services.

## 2 Developments in the Computing Industry

In this section, we first describe how surveillance capitalism has shaped the computing industry over the past two decades. We then argue that certain enabling technologies both emerged out of and feed into this development.

### 2.1 A Takeover in IT



In the aftermath of the dot-com-bubble (see (Zuboff, 2019)), the surviving IT companies had to find business models to provide the high rate of return demanded by the venture capitalists who funded them. In order to keep increasing the user base, it was essential for the services to continue to be free of charge for the end users (e.g., for Google, see Zuboff (2019)). Therefore, it comes as no surprise that they chose to embed advertisements to generate revenue. The way in which this was implemented was new, and it is not only the source of the profitability but also the origin of the problems that we will describe in Section 3. Instead of merely placing ads, user actions were tracked and recorded in large databases. Apparently investors and advertisers were convinced of the effectiveness of this behaviorist approach, based on the high market capitalization of these companies. This is of course not proof of its effectiveness, but it is at least an indicator. Most of the concerns with the practices of data gathering that we discuss throughout this paper remain true even if the real effectiveness of the attempted behavioral manipulations is lower than commonly assumed.

The takeover by capital interests is typical for IT services and has been repeated for many platforms that were created later. Because IT industries were the dominant source of innovation for the past two decades, the growing market attracted investors, and early pioneers matured into global businesses. For instance, Facebook began as a network to connect Harvard students, then developed new features and integrated other universities. After they needed money and found venture capital, their focus shifted increasingly toward profits. A set of tools were developed that aimed to maximize the users' receptivity to advertising. Similarly, Airbnb and Uber started out as platforms with the idea of making unused accommodation and ride capacity available for the financial benefit of the users. However, in the course of seeking additional profits, the relationship with these users changed to one in which they were exploited by the platform operators (Scholz, 2017).

## 2.2 Enabling Technologies

The success of this data-gathering business model required the development of infrastructure that was able to integrate a wide range of data sources and to store large amounts of data. After all, users have a range of devices and operating systems, and the amount of data generated was enormous. When the costly infrastructure was leased to other companies as a service, Cloud Computing was born. Amazon and Google were the first to open these extensive server structures, along with sophisticated programming environments and information on how to use them, to external companies and individuals as a separate profit-making business. In addition to Infrastructure as a Service (IaaS), which is still quite replaceable by offerings from other companies, they offer Platforms or Software as a Service (PaaS and SaaS). These services are less replaceable, and therefore come with a higher dependency by the customers. For all of these services, the

service providers have an interest in high standardization in what they provide to their different customers, thus optimizing for serving a large customer base at a small expense per customer. In some cases basic services are offered for free (Google Cloud) and monetized via the gathered data, whereas more extensive services are offered for a fee. The fee-based services are highly profitable for their providers — for instance in 2019 Amazon Web Services accounted for only 12.5% of the company's revenue but generated 63% of their profits (Sparks, 2020). The Cloud Computing market has an estimated turnover in the hundred billions of USD in 2020 (Richter, 2020).

The largest market shares are held by Amazon Web Services, Azure (Microsoft) and Google Cloud. Even though they found a business model that does not rely on advertisement and manipulation, all of these services are still based on a centralized data architecture and increase the power and reach of the surveillance capitalists. This is because they successfully established an infrastructure that an increasing part of the economy depends on: which companies that have integrated cloud services into their work flow are prepared for the case that their service provider would suddenly deny the service?<sup>1</sup>

In addition to storing the data, its effective evaluation for monetization required new kinds of algorithms. Targeted advertisements and other means of adaptive functionality are based on the evaluation of all the available personal data. In addition, particularly for social media platforms, desired functionalities such as page ranks, news feed algorithms and content moderation require a certain degree of individualization. All of these would be much too costly to do manually; the desired individualization conflicts with the standardization and uniformity of the scaling big imperative. This conflict was reconciled by using Machine Learning. While Machine Learning has existed in some form for decades, these centralized and data intense platforms offer vastly more data and opportunities to train neural networks, along with an application domain and funding to enable an explosive growth in research and development in this area. Page rank, natural language, and (facial) image recognition are only three areas of success for these algorithms. Basically, whenever these corporations need to make sense of vast amounts of data, this type of Machine Learning seems to provide a crucial technique for the business model.

The trends of the last decade in the computing industry are therefore intertwined with the large IT companies' orientation towards surveilling their users and commercializing the resulting software and infrastructures. They have been driven precisely by these companies and have helped them to succeed. Only later were the tools opened up and applied to a wider range of problems. In particular, targeted advertising created the foundation for a certain paradigm in the IT industry that can be called surveillance-based computing. This process again strengthened the big IT companies. Language recognition is a perfect example

---

1 See the case of Parler in January 2021.

showing how the functionalities which the business model evolves, when adopted, feed in even more data into the data silos. For instance, many people allowed (even paid for) an Amazon or Google device to record them continually in order to benefit from voice controlled services. Another example is face recognition, which makes cameras a significantly more powerful tool for the end user, thereby incentivizing their usage, which yet again feeds in more data. (They are of course at the same time a significantly more powerful tool for surveillance.) Therefore, both Cloud Computing and significantly more powerful implementations of Machine Learning emerged out of this particular business model, and further enhanced the service providers' position as surveillance capitalists. As we will discuss in Section 3, this development has resulted in a very harmful direction for the entire IT industry.

### 2.3 Retaining the Benefits

Despite the very dark sides of surveillance capitalism, at the same time these services are sophisticated in a technological as well as in a usability sense. They have enormous utility for business, social engagement, political work, and much more. So in any potential approach to address these problems, we want to retain as much as possible the benefits. Instead, regulations should address the dominant business model and allow for different technological paradigm to flourish. With different business models we will hopefully see a different computing paradigm and thus different innovations emerging from it. In this way, political regulation should impact the direction of the IT industry.

## 3 Problems for Democracy and Sustainability

In this section we discuss the processes by which surveillance capitalism impacts consumerism, threatens democracy, fuels social fragmentation, undermines our ability to tackle the major environmental problems and thereby ultimately constitutes a hurdle to any sustainable development within the planetary ecological limits. While workers in leading positions in those companies were well aware of their influence on human behavior and the negative effects on society (Allen, 2017; Murphy, 2017), it was underrecognized by major parts of the society.

All problems that we identify originate from at least one of two sources. The first one is the aforementioned business model. The second one is the central control over the software and data architecture that we make ourselves dependent upon. We need to distinguish between these sources, and though both are problematic, we suggest that regulation (Section 4) should start with the business

model — the root cause — instead of the enabling technologies. We first discuss both of these sources, and then describe the resulting problems, which we cluster into sustainability aspects (Section 3.2) and political aspects (Section 3.3).

## 3.1 The Root Causes

### 3.1.1 The Business Model

The business model (of free services that monetize user data) produces a range of problems. In order to maximize the value for advertisers, the companies need to capture the user for as long as possible on the website or using the application. This effort is supported by applying knowledge of human psychology (Matz, Kosinski, Nave, & Stillwell, 2017) and by experimenting with different interfaces using A/B and other testing. (Another more publicized example is the Facebook emotional manipulation study discussed in Section 1.) One strategy to maximize the time spent on social media is to push toward more provocative content, both on the side of the viewer (who becomes more engaged or outraged when confronted with extreme positions, so that feeds tend to select for such content (Tufekci, 2018)), and also on the side of the contributor (since these posts then tend to receive more positive feedback, encouraging users to post more in that direction). This self-enforcing feedback loop is just one example rooted in the basics of human nature. Other strategies are to trigger anxieties or fear (fear of missing out, or how one compares with others). Overall, these methods aim to result in a strong pull toward the website, platform or application. In addition to maximizing the number of people who see an advertisement and the length of time they attend to it, the ad also becomes much more effective if seen by groups most likely to respond to it. IT companies that gather personal user information can not only identify the users as participants of a certain group, they can also use their elaborate algorithmic tools of statistical analysis to identify for the advertiser which target group to aim for (Buettner, 2017; Matz et al., 2017). However, in order to provide these services to the advertiser, the company needs to gather and correlate more and more personal information.

There are four phenomena taking place simultaneously. First, the companies are gathering any available possibly relevant raw information by tracking the user, including actions taken in the browser, contact addresses or the mobile location. In addition, if the records that belong to a given person can be connected during a series of visits and between different websites or applications, a far more sophisticated user profile is generated. This is the reason these websites use trackers that are able to track the entire activity during the browser session. It is also a reason that Facebook and Google are highly motivated for users to use their Facebook or Google accounts for identification with other service providers. Third, the correlation of many of these sophisticated user profiles makes it

possible to make statistical predictions about user behavior, and thereby make sophisticated assumptions that are not even necessarily limited to what the users themselves are conscious of (Dufner, Arslan, & Denissen, 2018). Because of this intra- and inter-personal connection, new data is more valuable the more it can be correlated with already-held data. As a consequence, a network effect occurs that amplifies the centralization of data. A fourth possible practice that is becoming increasingly relevant is the manipulation of user behavior on the basis of that data. A detailed knowledge of which environments a given user can be most usefully exposed to, to increase the probability of a desired behavior, leads to a whole new category of customers, since in addition to classical product advertisement, the companies can offer political influence, particularly in general elections (Vengattil & Dave, 2018; Vines, Roesner, & Kohno, 2017). If the desired user reaction is no longer limited to buying a certain product, but also to nudges toward adopting a certain political opinion or voting in a certain way, the IT companies have deployed a tool to help wield power and control over society. This shift from merely advertising goods and services to political influence would only be accelerated by a regulation that tackles merely the commercial advertising part. We do not attempt to quantify in this paper to which degree these companies have already performed this shift. The point is, instead, that they have the incentive to do so and that is highly problematic.

### 3.1.2 Surveillance Computing

In every industry, service providers have an interest in retaining their customers and serving them at the lowest possible cost. For Cloud Computing providers, this means on the one hand keeping the (technical) hurdles high for emigrating with data to another service provider, and on the other hand achieving a high level of standardization. Both have a centralizing effect.

Centralized data is highly suitable for training neural network based Machine Learning algorithms. The behavior of these algorithms is largely determined by the training data and the function that evaluates the responses of the algorithm. Why exactly the algorithm comes to a concrete answer and how valid is this answer is typically a black box even for the developers. While real world problems are typically structured in more complex manner, in some application domains AIs beat even the best human experts, e.g., games such as chess or go.

When algorithmic results support social practice, a major problem arises with trusting the outputs of these AIs. Through the choice of training data and the evaluation functions, biases are introduced in the algorithms, which then become firmly anchored in the AI (Osoba & Welser IV, 2017). For example, if legal decisions or online censorship were to be made by an AI, any (unconscious) discrimination that this AI has would be reflected in these decisions: first, discrimination in the cases used as training data, and second, random correlations between the characteristics that should be tested and other characteristics that

should not influence the decision. In a sense, neural networks take the biases from the past and entrench them into the infrastructure of the future.

What Cloud Computing and Machine Learning share is that they do not function locally. Whereas in the past software, once it was developed, was installed and used locally, today we see a different pattern. To access one's data in the public cloud or to use an AI algorithm, it became common practice that the data storage and processing takes place at a central server structure, distanced from the locality of usage (although, once it is trained, it would be possible, to apply and even adapt the AI locally). As a consequence there is a dependency not only on a permanent online connection but also on the service provider. This dependency results in a position of power for the service providers.

Above we suggest that the current business models have a specific effect on the orientation of these IT companies; in particular, it leads to intensive gathering, tracking and correlation of personal data. We also argued how this is the basis for Cloud Computing and recent Machine Learning results, and how these have a power centralizing effect. We categorized Cloud Computing and Machine Learning as enabling technologies, because they emerged from and feed into surveillance capitalism. Simply discarding these technologies (and it is questionable how desirable that would be) would not solve the problem of surveillance capitalism. Nonetheless, they do magnify the problem, by providing both a greater incentive and new ways to collect data. In addition, we see Cloud Computing as another locus of control that surveillance capitalism moves into. The currently dominant loci of control can be considered to be mainly the free services of social media and browsing. They are both the battlefield and the weapons with which surveillance capitalists fight for influence. As we will argue, the area of Cloud Computing can be expected to follow a similar pattern.

In the following section, we further explore the outcomes for individuals and society. This helps us to illuminate how these developments in the computing industry pose a threat to sustainability and democracy in multiple dimensions.

## 3.2 Sustainability Aspects

### 3.2.1 Consumerism and Excessive Consumption under Conditions of Relative Saturation

Western economies have reached a stage that Keynes (1971) called endogenous growth weakening. He postulated in highly developed economies a relative saturation of peoples' needs, in the sense that owning a 3rd or 4th TV set or mobile phone would not create much more additional satisfaction for consumers. Therefore, growth rates would decline and these economies would tend to stagnate. Following the post-war decades of fast growth, since the 1980s Western economies have experienced rather low growth rates on average (Zinn, 2009).

Under the conditions of relative saturation all means that can stimulate consumption become very valuable. The high stock market value of platforms whose economic models incorporate elements of targeted advertisement seems to support this assumption. The increasing effectiveness of customized advertising (even if only a modest increase) fuels the imperative for consumerism and unending growth. A market-based economy is founded on the idea that people's needs, expressed through demand, result in a corresponding adjustment of supply and thus increase the quality of life. A problem arises when the relationship is reversed, and companies try to manufacture demand to match their supply. The increasing forms of targeted advertising aimed at individual psychological susceptibilities are one means of artificially creating this demand. While this generation of artificial needs is valuable to the advertising companies that can serve them, it has a destructive influence on individuals as well as society as a whole.

On the individual level the users pay twice for these artificially generated needs: once with the money they spend on their purchases, and also with the time they spend due to the provocative content and in psychological traps. On the level of the overall system, the practices of targeted advertising and intended manipulation work in a twofold way. First, they act in a fashion that is antithetical to the sovereignty of individuals that is necessary for an intact democratic process (as we discuss in the following section). Second, these practices represent a way of continuing to support the life of an economic system that requires continual growth, in a time of relative stagnation (in the West) (Zinn, 2009). The cost of this is a path, that if continued, will exceed the limits of liberal democracy and also for quality of life on this planet.

### 3.2.2 Consequences for Sustainability

The concentration of power in a small number of IT corporations is followed by a concentration of wealth (as can be seen by the amount of capital these companies have been able to accumulate). In other words, this development in the IT sector enhances the concentration of power within and outside these IT companies. Furthermore, the small number of employees versus the revenue generated by these companies exacerbates this effect. While the funders and venture capitalists made fortunes, at least in the cases of Facebook, Google and Amazon, the most power resides with their founders, who have specific voting rights that give them additional control over their companies (Zuboff, 2019). The resulting increasing inequality undermines sustainability, democracy, and much else.

Even more important, the kind of growth that is stimulated by the above mentioned forms of advertising does not take place in any productive way. The increased consumption of the advertised products is an ever faster conversion of

valuable resources into waste, which is then dumped into the environment: the system in which the advertised products circulate is far from a circular economy.

Furthermore, we believe that living sustainably demands qualities that are similar to those required for the democratic process, thus many of the arguments we make in the following section also have sustainability implications. Challenging the worldview of humans as objects for extraction via targeted advertising, and also tackling the global challenge of a transition towards a more sustainable economy, will require information and energy channeled in that direction and significant personal perseverance. We do not see that the practices that social media platforms incentivize (for example, attending to short bits of information and multi-tasking, rather than concentrated thought about a complex, long-term problem), contribute at all to the focused pursuit of long term goals (even if this is yet under-investigated).

### 3.3 Political Aspects

#### 3.3.1 Three Dimensions of Power

We have already noted how the control over the infrastructure our society uses creates a strong dependency and thereby centralizes power in the hand of these companies. Even if this power is not (yet) used to extract wealth by charging (higher) fees for the use of services, it is exercised in other ways. We conceptualize these ways as three dimensions, which we will consider in more detail below.

- (1) Service providers can be selective and refuse services to users who are overly opposed to their own interests.
- (2) Service providers can surveil their users or evaluate metadata for monitoring purposes.
- (3) States or their secret services (especially those where the service providers are located) can gain access or use the platforms themselves to enforce sanctions.

Many problems touch upon more than one of these dimensions. For example, an effective censorship regime relies upon intelligence information regarding whom to censor and therefore requires some kind of surveillance. Nevertheless, these dimensions can serve as a useful conceptualization. Principles that help protect against the threats embodied by these three dimensions can be considered to be (1) freedom of speech, (2) privacy, and (3) independence from political manipulation. Yet, as we will see in Section 4, a response should be more nuanced than an absolutist version of these principles (e.g., free speech absolutism).

However, every instance of using this power would also make the service provider less attractive, which might be a problem for them if there were



significant competition. But with the current monopolistic market situation, the scope of action of the economic actors who have made themselves dependent on the service providers is severely restricted. Even just the threat of some punitive action by the service provider, even if never actually carried out, shapes their actions. Further, for an individual user, the potential negative consequences in the future resulting from the use of these services is difficult to anticipate. This is clearly not supportive of making well-informed decisions.

It appears that for social media, browsing, and similar services, currently the second dimension (invading privacy) is most profitably turned into revenue (by predicting and manipulating user behavior), whereas for cloud computing the primary portions of the service are provided for fees. However, these circumstances may change in the future, especially when the degree of dependence has increased.

We will now discuss these three dimensions in more detail.

### 3.3.2 Free Speech and Participation Dimension

Social media platforms such as Twitter, Facebook, and Instagram offer new types of (semi-)public spaces. They play an increasingly important role in the exchange of ideas, visions and convictions that drives the necessary continuous adjustment of the overall political picture. However, the (mostly machine learning) algorithms by which content is selected are often opaque to the reader (Ávila, Freuler, & Fagan, 2018). Further, these public spaces can have an emancipatory effect specifically under the conditions of surveilled telephone lines and censored mass media, as occurred in the early stages of the Arab Spring when discussions critical of the regime, planning for demonstrations, and the distribution of news was facilitated by these platforms (Rohde et al., 2016; Wulf, Misaki, Atam, Randall, & Rohde, 2013). Precisely because these spaces are semi-public, however, no legal protection of freedom of speech is in effect. Freedom of expression therefore depends simply on the decisions of the service providers.<sup>1</sup> This limits their emancipatory potential; and certainly a small number of unelected, extremely wealthy individuals should not have that sort of power over a democracy.

While a selective refusal of service would not be a problem in an ordinary service market situation, it becomes problematic at the point where economic or political operators have made themselves dependent on the infrastructure — the semi-public space is privately owned. At that point, this refusal functions as censorship or sanctioning. Amazon (a semi-public market space) can for example simply exclude certain sellers who do not deliver the information they request. Another phenomenon of recent years is the possibility for people to earn a living

---

<sup>1</sup> Consider for example the deactivation of Donald Trump's Twitter and Facebook accounts in January 2021.

by some kind of informational or entertainment content they present at online platforms. For instance, YouTube and Twitch are particularly suitable for that, and Patreon actively promotes this form of self-employment, whereas Facebook and Twitter are more used as an outreach to people. This form of self employment is particularly vulnerable to sanctions from service providers. In particular, when as a result economic autonomy and political opinion interact, it becomes highly worrisome.

The next level would be Cloud Computing services acting similarly against their customers. Here the barrier to this happening is a little clearer, since such measures would directly (although slightly) cut into their own revenues. Yet again, the potential threat of such measures oftentimes results on self-imposed limits on the businesses that use the providers. In particular, small and medium-sized companies tend to make themselves dependent upon cloud services without including these dimensions of power in the calculation. A notable politically charged case occurred in January 2021, when Amazon Web Services used this power against one of its customers, Parler (a social media platform more tolerant of posts urging violent action than for example Facebook). As a result, Parler in effect had to go out of service. While we may be thoroughly unsympathetic to Parler itself, this prospect is worrying, not least because today a significant proportion of businesses would already be crippled by a refusal by their cloud service providers to do business with them.

A more nuanced but not less relevant form of the censorship category applies to navigators in the (virtual) world, such as search engines, news feeds, and to some extent even maps and public transportation information. The service providers control which parts of these virtual semi-public spaces are visible to the user and which are omitted, oftentimes controlled by Machine Learning empowered algorithms. By selectively distorting the perspective, the operators of semi-public places can try to influence behavior, including the political beliefs of the users.

These concerns also apply on a geopolitical level. Whereas in the past, concerns with for instance the EU depending too much on infrastructure from the US could be downplayed as they are considered allies, in 2020 we saw the US sanctioning EU companies for building a pipeline in the Baltic Sea (Hackenbroich & Leonard, 2019). Given that sanctions are already an escalated step in the enforcement of political power, these concerns are increasingly justified. Any dependence upon centrally controlled infrastructure makes actors vulnerable to sanctions, and even the possibility of these sanctions weakens one's political bargaining power.

### 3.3.3 Privacy Dimension

The second dimension becomes relevant in all cases where data is uploaded unencrypted to online platforms or service providers.

At a business level, semi-public spaces create the illusion of effective markets. The principal but highly concerning example is the behavior of Amazon, which surveils not only the shopping behavior but also the sales behavior on the platform. In case Amazon discovers that certain products are particularly profitable, they offer these products themselves. The fact that they own the semi-public marketplace places them in an unfairly advantaged market situation.

At the level of social media, the content of discourses will be recorded by the platforms and can contribute to the personal profiling of the discussants. Thus, the semipublic spaces have a Janus nature. They offer emancipatory potential, but at the same time contribute to the refinement of personal profiles and opportunities for manipulation. The role of Facebook in the 2016 U.S. election and the appropriation of the Whatsapp messenger in the recent elections in Brazil shows the manipulative power that comes with the ability to create personal profiles and to distribute targeted political propaganda via social media platforms (Kaiser, 2018; Swearingen, 2018).

The practices of personal data amassing conflict with principles of privacy. Although people deliberately choose to use the services and thereby provide their personal data to the company, they are pushed to do so, due to a lack of transparency regarding which data is tracked and to whom it is given, with little understanding by most users as well as the non existence of real alternatives or options for end user control. While general business conditions or national law may regulate the handling of this data, (a) this regulation is only on a legal level, whereas misdemeanor can be hard to prove on a factual level (How should a citizen prove that a company is hiding something in their data silos to which they have no access?) and (b) these regulations do not apply to predictions generated from this raw data.

A lack of privacy with regard to political communication on social media platforms can lead to less participation and to self-censorship, depriving the debate of opinions that could support political progress. Particularly due to the potentially unlimited lifetime of the data, and lack of transparency with regard to what personal data was gathered and how it was used in profiling, people in public offices or running for them will have to permanently fear that unpleasant private matters from their past could be dug up. In addition, the pressures toward more and more provocative content drives extremism and social fragmentation.

Looking, for instance, at the experiences of the Arab Spring (Rohde et al., 2016; Wulf et al., 2013), it becomes obvious that authoritarian regimes can use the personal data stored in social media platform for surveillance and propaganda. This facts applies unfortunately also to Western governments (Snowdon papers). The platforms themselves do not need to be in hands of the government; it is

sufficient for the government to gain access to the gathered data. As the case of NSA indicates, platform providers could grant the access if they are blackmailed by legal action or threats of losing government support or even market access. A state does not need to initially be an authoritarian regime to develop in that direction. But even for a working democracy, these types of surveillance techniques are concerning.

### 3.3.4 The Dimension of Independence from Political Manipulation

One response to these problems could be government oversight to ensure that the services are at least not used against the interests of their own citizens. However, government oversight or control leaves open dangers of political manipulation. Therefore, we treat this as a third dimension in the exercise of power that should be considered.

In China, the government is actively accessing and censoring different social media platforms, and at least intends to profile the behavior of its population by means of a point-based social credit system (Chen & Cheung, 2017). In the west, this is regarded as a development toward an Orwellian surveillance state (Chin & Wong, 2018), while at the same time similar software architectures and personal profiling capabilities are built up. Although in the west the state is not yet (legally) able to directly access these profiling data and match between the different platforms, security services seem to have these abilities. Even in western democracies, governments will not want to see any drift toward political opinions that do not support their own political mandate. If they, instead, can use these services as a tool to propagate their own world view, it could in the eyes of the government even be a good thing to do so. Therefore, it comes at no surprise that many countries deploy significant resources to manipulate domestic as well as foreign public spaces (Bradshaw & Howard, 2017).

Particularly in democratic countries, the targeting of voters based on their psychological profiles becomes politically charged, as the case of Cambridge Analytica shows. This company was involved in the Brexit referendum as well as in the Trump election in 2016 (Cadwalladr, 2018; Manokha, 2018). In addition to these attempts to influence how citizens vote, the possibility of running for office is threatened as well. When it is fully opaque to people what information about their past is stored somewhere and might be unearthed to defame them, running for election may become daunting.

The combination of these developments is particularly worrisome. For example, when facial recognition made possible by Machine Learning is combined with cameras in public spaces and profiling from social media, a powerful surveillance apparatus is created. Another example that Tristan Harris, Cofounder of the Center for Humane Technology<sup>1</sup>, points out is the application of

---

1 <https://www.humanetech.com/technologists#principles>

Machine Learning to the algorithms of social media content filters. The kind of artificial intelligence that has allowed computer programs to win against the best chess grandmasters is used today to capture the attention of users. Although this comparison is limited — capturing attention is neither an evenly matched game, nor is it as suitable for AI as is a narrow problem such as chess — social media users may not even know what the platforms are doing to attempt to capture their attention. These practices oppose the autonomy of the people.

Once the sovereignty of humans (over their personal data and their well informed choices grounded in their social practices) is at stake, the borders with a propaganda and surveillance state blur. Or as the Cambridge Analytica whistleblower Christopher Wylie puts it (Cadwalladr, 2018):

*If you do not respect the agency of people, anything that you're doing after that point is not conducive to democracy.*

### 3.4 Surveillance Capitalism Undermining the Foundations of Society

So far in this section, we have described the effects of these business models that are based on massive data gathering. These effects can be summarized as undermining the foundations of democratic society, and further strengthen government control in authoritarian ones. They also contribute to an existing trajectory of an unsustainable economic system that disrespects planetary boundaries and thus undermines foundations of human life on earth. In brief, an unregulated (surveillance) capitalism is destroying its material and political foundations.

On the basis of this analysis, we can now sharpen the picture of surveillance capitalism. The core of surveillance capitalism lies in the control over infrastructure; In Zuboff's terms it is the infrastructure which is capable of generating predictive and manipulative capital. This is a form of capital, but one that does not add to the quality of life, but instead undermines it. Free services monetized by targeted advertising is only the current variant in which surveillance capitalism plays out. However, the core problem lies neither in the advertising nor in offering the services for free, but in using the control over the infrastructures that our society increasingly depends upon, married with intensive gathering and cross-correlation of personal data, against their own interests. To the degree that service providers for e.g. Cloud Computing apply these practices, in spite of partly having a different revenue model (paid services), they are still surveillance capitalists. With this sharper picture of surveillance capitalism we can make an analogy and derive a prediction. In the same way as for the civil society free IT

services play an increasing role (e.g., by the influence of social media), the economy is increasingly shaped by Cloud Computing. And although the negative effects of Cloud Computing are not as apparent as for free services yet, we argue that Cloud Computing is the next upcoming locus of control where surveillance capitalism will be fought out.

Note that none of the problems is entirely new. Strategies to influence human behavior are at least as old as civilization; the same is true for the exploitation of nature for human consumption. Morozov (2019) also rightly notes in his critique of Zuboff that capitalism has actually been working in the same way for a long time: “To view surveillance capitalism as our new invisible Leviathan is to miss how power, under capitalism, has been operating for several centuries.” However, what we do claim is new is that now tools exist to implement these strategies (e.g., manipulation of political convictions) on a larger scale and with fine-grained targeting based on detailed knowledge of individuals. The question must therefore be what to do about these powerful tools.

## 4 Possible Solutions

Turning now to what could be done, one goal should be to limit the damage done by the surveillance capitalism business model, while still retaining key benefits of the services it provides. But if possible, we would like to move beyond damage control, and support positive visions of how IT can better support people and communities. Crafting and deploying such solutions is an exceedingly difficult problem. Even though this business model has only recently come into being, the corporations practicing it have become dominant, and the technologies and services are threaded throughout our lives, communities, and economies. The ideas presented here are incomplete, and we welcome the opportunity to engage in dialog about what we as a society can do. Regulation will be a key element of a response; but a common thread in this section is that regulation should be co-designed and co-evolved along with the technology and accompanying social practice, rather than simply being a reaction to technology and an attempt to curb its worst excesses. Another common thread is that this is not at its root a technological problem amenable to a purely technological fix.

### 4.1 Regulation and Law

Regulation and law form key elements of possible solutions. We suggest three principal goals: protecting privacy, erecting barriers to behavior manipulation, and undermining the economic basis of the surveillance capitalism business model so that alternatives can take root and flourish. Having such alternatives should lessen

the dependence on these IT companies, while still having a way that people and society can have access to useful IT services — and beyond this, support positive visions of the role of IT in communities and society. These proposals thus address the dimensions of participation and privacy noted in Section 3.3. The proposed regulations undermine the surveillance capitalism business model and thereby erect barriers to behavior manipulation.

The General Data Protection Regulation (GDPR) from the European Union, which took effect in May 2018 is certainly a major step forward for protecting privacy. In spite of its limitation to the EU, the European user base is large enough that this is having a meaningful influence on the behavior of the major corporate players. In some cases, the service providers may simply apply the same technology globally; in others, the EU experience may inspire similar regulatory efforts elsewhere. Under these circumstances, the EU could not only lead the way in regulatory terms, but even be in a position to set data protection standards for users worldwide. While this is a positive prospect, it also means that the EU's legal space can be expected to be particularly competitive. This is because the companies most affected by this will be able to afford to hire numerous highly skilled lawyers, lobbyists and others to protect themselves against any negative impact on their profits. Furthermore, if the result of such regulation is merely requiring users to give consent, it is not particularly helpful unless there are meaningful alternatives they could switch to.

Another area of legislative activity is do-not-track legislation, which aims to strengthen users' rights not to be tracked by third parties while browsing websites and potentially while using other internet-based services. In the US, a series of such bills have been introduced, ranging from the Do Not Track Me Online Act of 2011 to the Do Not Track Act (Hawley, 2019). The general goal of these bills is to allow users to decide whether or not they are willing to be tracked by third-party websites. These bills certainly are steps in the right direction, though international agreements would need to expand this to similar legislation that apply to both users and companies internationally. There are also numerous important other considerations, such as what the corporation that is offering the given service can track (as opposed to a third party), and whether there are mandated default settings to not track.

#### 4.1.1 True Informed Consent

One reaction to privacy concerns is to implement much stronger requirements for informed consent, of which the GDPR is one important example. Improving information and consent is certainly a good thing, but in our view is inadequate. Being deluged with pages and pages of consent agreements about what information is being gathered about you isn't that useful, and if the alternatives are to check the "agree" box, or to be left out of a great deal of social and political

interaction, this is not a particularly meaningful choice. However, stronger implementations of consent are possible.

As a thought experiment, suppose that surveillance capitalist corporations were required to operate under the same conditions that govern research involving human subjects. For example, in response to past abuses, the US government adopted the Belmont Report (1978), which laid out principles for human subjects research. It requires true informed consent, which must be voluntary and ongoing. That implies that the consent form must be straightforward and comprehensible — so no 30 page legal monstrosity as with typical corporate privacy statements — and the subject must be able to withdraw from the experiment at any time. Further, only data needed to conduct the study should be gathered, and must be deleted once the study is over and analysis is complete. The data must also be held confidential and protected — it would be forbidden, for example, to hand it over to another research group without consent.

If similar requirements were placed on surveillance capitalist firms, they would require true informed consent, the ability to withdraw one's data at any time, and would not allow the data to be shared without permission with a third party. People should be able to challenge inaccurate information and have it removed. Note that today people do not even have access to a transparent overview of how their private data is trapped, transferred, sold and aggregated. Therefore, as a prerequisite, these data pathways need to be visible for the user and the public regulators.

Further, in analogy with the human research requirements, only the data needed to provide the service in question could be gathered, rather than the cloud of additional data that is gathered and retained as at present. In other words, what we advocate includes (but is not limited to) “minimum data.” These corporations should not be allowed to collect data that is not necessary to provide their service. However, minimum data alone could still leave loopholes for service providers, e.g., they could claim all personal data collected is necessary for AI-powered algorithms to provide a service optimized to personal needs. Therefore, true informed consent in analogy with human research requirements exceeds the minimum data approach. Finally, the requirements should be much stronger for children and vulnerable populations (e.g., prisoners). For example, in many cases the companies should simply not be allowed to accumulate information on children.

Again, this is just a thought experiment — wishful thinking, perhaps — but is intended to show how regulation might more meaningfully support privacy in these services.



#### 4.1.2 Adversarial Interoperability

So far, we have addressed the privacy dimension that was identified in Section 3.3. But meaningful regulation with respect to the other two dimensions is possible and necessary. Solutions that help with the first dimension (free speech and participation) require the availability of meaningful alternatives. These are not present in the current IT landscape, which is dominated by companies in relative monopoly positions. Breaking up the monopolies would be a useful step in ensuring that users are not too dependent on their service providers. However, more is needed. In our view, simply splitting Facebook, for example, into 6 mini-Facebooks, each with the same surveillance capitalism business model, would not be sufficient. It also makes sense to break up companies along functional lines, and to regulate the exchange of information among these now-third-party entities. For instance, Facebook could be required to divest from the essentially unrelated parts of its business, including Facebook Messenger, WhatsApp, and Instagram. However, just doing that, each sub-company could hold the monopoly in its niche, so a comprehensive approach must go further. And given the network effect and the centralizing aspects mentioned above, which is prevalent for Internet platforms, reverting to a monopoly situation is the most likely outcome without additional regulation and oversight.

Interoperability is one key to reducing the user's dependence on the corporation or organization providing the service, as well as increasing the ability of small competitors to improve upon single features. In his recent book *How to Destroy Surveillance Capitalism*, Doctorow (2020) uses the term adversarial interoperability, capturing that interoperability cannot be expected to be voluntarily implemented by for-profit companies. However, it would make it easier for for-profit competitors to enter the market, as well perhaps as nonprofit or public entities, and therefore should be legally enforced. Doctorow argues: "If our concern is how corporations are foreclosing on our ability to make up our own minds and determine our own futures, the impact of dominance far exceeds the impact of manipulation and should be central to our analysis and any remedies we seek." His position that enforcing antitrust legislation in this domain is an important one, although we would add that protecting against surveillance and manipulation is equally important.

Antitrust law may provide a suitable means for motivating requirements for adversarial interoperability. We are not experts in the law, but we can say that it will probably not be enough to apply existing antitrust law consistently to the case of IT services; new regulations will also have to be added. For example, antitrust law as currently interpreted aims at enforcing fair prices for customers. This does not cover the case of free applications, in other words, the users who should be protected are not even the customers in this case.

Since these measures directly attack the power position of IT companies, countermeasures are to be expected, including extensive lobbying and media

campaigns, as well as the continuing instrumentalization of intellectual property laws. For example, even if an IT service were involved in the creation of content, it should not be granted any intellectual property rights. Otherwise, Facebook, for example, could prevent users from scraping their content and uploading it on a competing system. The same is true for Cloud Computing providers. Therefore, IP restrictions are quite consequential and must be considered to in responding to the expected countermeasures. However, intellectual property is just one way in which law is used to create abstract forms of capital. In her recent book *The Code of Capital*, Pistor (2020) shows how the law selectively codes claims and ideas into capital. All of these forms need to be considered as expected legal countermeasures big companies will apply against regulation.

#### 4.1.3 Consequences for the Business Models

The regulations we suggest would significantly challenge the surveillance capitalism business model and help to foster alternatives (see the discussion below). Let us there fore consider which business models would still be possible under such a regulatory regime.

We can conceptualize the evolution of the business models that have led to surveillance capitalism as taking place in stages. There is a stage of broadcast advertising with a general audience, followed by a stage of context specific advertising (this would include advertisements based on the current behavior, such as the terms entered into a search engine). A third stage is targeted advertising (this would include personal profiling), and a fourth stage is targeted manipulation that is not limited to advertising consumer products but includes influencing political opinions and actions (see Section 3.1.1). The shift from context specific to targeted advertising marks the location of a suitable line to draw and challenge surveillance capitalism by prohibiting advertising based on personal profiling. However, targeted advertising is not the only way in which the control over the infrastructure and personal data can be turned into power over people. Even if the advertising portion of it were to be dropped completely, all three dimensions of the political problem would persist. Prohibiting targeted advertising makes the monetarization more difficult and thereby reduces the incentive to gather this data. Yet, it does not address the full problem. Our suggested directions for regulation, grounded in true informed consent and adversarial interoperability, would make targeted advertising as a basis for business untenable, but that is not the only issue. This regulatory direction is also more adequate to deal with an expansion of the arena in which surveillance capitalism is played out (from free services to offerings such as Cloud Computing), as discussed in Section 3.4.

Precisely because the proposed regulations challenge the power of the tech platforms directly, we should not expect them to simply comply. Investigations

and whistleblowers will be necessary for identifying misconduct. As a consequence, there should be compensation paid, and since one of the aggrieved parties is society as a whole, it is easily justifiable to channel this compensation into the development of alternatives, as one source for funding for them.

The business models that are still viable under such regulations include for instance traditional (context specific) advertising and paid services. This would help avoid undermining services whose business model does not rely on behavioral manipulation, the highly profitable Cloud Computing business being one example in this category. The benefits from the enabling technologies can thus be preserved while liberating them from their role as surveillance capitalism suppliers.

## 4.2 Some Limitations of Regulation and Rejected Approaches

In the ongoing public discussions about problematic developments in the IT industry, a variety of approaches have been proposed. However, we regard a number of them as insufficient. In this section we argue why we think this is so.

One approach that seems inadequate is to model private data as a good to which people have property rights and can sell. The idea is that users could then benefit from the profit made on their data. However, most importantly, fundamental rights, such as privacy, should be above the market and not embedded in it. In addition, people would receive little for their data, due in part to the asymmetric market situation. Finally, none of the problems discussed would be addressed by this approach.

More generally, the whole approach of treating data as something that can be owned seems fundamentally flawed. When data is created by an amalgamation of different technologies and people it is questionable who the owner should be. Furthermore, as information, data can be copied and processed arbitrarily. If various data sources are processed into further data using analysis methods, who would have ownership claims over them? If a company is required to delete certain stored data X or not to use it for certain purposes, that company cannot prove beyond doubt that it is actually complying. Even if it were to disclose all its data and give details of its origin, it could still hide the fact that some derived data actually originated from X. It would only be possible to prove a violation, e.g., by a whistleblower. Simply put, the data ownership approach that treats information as if it were a physical object seems ultimately infeasible. However, Hummel, Braun, and Dabrock (2020) argue that it misses the point to reject claims for data ownership on the grounds that property in data does not exist. Instead, claims for data ownership should be understood as attempts to call for the redistribution of material resources. Furthermore, Duch-Brown, Martens, and Mueller-Langer (2017) analyze how the concept of data ownership leads to data market failures.

But these considerations bring out some limitations even for the privacy-preserving approach that we suggested. Take the example of a photograph

showing a group of people at a particular location. Who should have which rights to the data? The stakeholders include not only the people in the photo and the photographer, but also the owners of the location and perhaps even the owners of the device used to produce the photograph. Furthermore, what is revealed about the different people if the picture is published? If the data involves several people, who can require that it is deleted and how do they prove their right to request the deletion? Do they thereby need to contribute even more personal data?

These considerations show that ultimately no regulation can do perfect justice to the protection of privacy. The inevitable legal inadequacies, as well as the impossibility of perfectly protecting against eventual data leaks, are both strong indicators that many data should better never be gathered in the first place.

A central feature of many proposals for regulating social media is content moderation. In our view, some content moderation is necessary: for example, social media should not allow child pornography or live-streaming mass shootings. Nevertheless, we should keep in mind that Facebook's algorithms, which tend to incentivize for extreme content, exacerbate existing social problems and divisions, but don't cause them to spring into existence from nothing. And overall, content moderation has significant limitations. For example, political truth can be hard to pin down. Putting the requirements for content moderation on the tech companies will likely stifle smaller companies entering the field (Doctorow, 2020). Furthermore, the companies might over-censor to be on the safe side, or use content moderation to censor arbitrarily according to their own agenda. In a quasi-monopolistic situation for social media, we view it as unacceptable that private companies can determine who can publish what (e.g., Twitter and Facebook closing down Donald Trump's accounts). So indeed, we need some content moderation to curb extreme content. However, content moderation alone will not be sufficient to tackle the problems of surveillance capitalism and social media, and in some ways is a red herring that distracts us from the real problem: the business model and its consequences.

Removing the financial incentives to present more and more extreme content to get users to spend more time on site, along with some content moderation in extreme cases, should go some distance toward improving the information that many users see in their social media feeds and that show up in response to searches. However, particularly in the current political climate, wild conspiracy theories and factually false information will almost certainly continue to circulate. We don't see an easy response to this issue. In particular, content moderation is not the primary answer; further, content moderation probably becomes more difficult if monopolies such as Facebook are broken up. Instead, we view these problems as arising in considerable part from the rising distrust in authoritative sources in medicine, science, politics, journalism, and other realms, coupled with a lack of skill, or a willful disregard, for critically assessing the reliability of information. Repairing this distrust and lack of critical assessment will not be

easy, but is essential. Among other things, it is important to recognize that outlandish conspiracy theories are more likely to thrive when there is a great deal of distrust in general, along with a considerable number of what we could classify as actual conspiracies (for example, among the ultra-wealthy to evade taxes by offshore shell corporations). Another ingredient in this restoration may be public funding of institutions (e.g., journalism), in order to remove conflicts of interest.

### 4.3 Social Practice

We have suggested that regulation should be co-designed and co-evolved along with the technology and accompanying social practice. Social practice can of course not be designed and imposed in the same way that regulations can be, nor would we want to be so arrogant as to suggest that this be tried. Nevertheless, social practice evolves and is molded in part by education, regulation, economic forces, and other influences; and we can investigate how these interact, and design technology and regulation to support positive social practices and underlying values. And as members of society ourselves, we can advocate for and model the social practices we think will have positive effects.

#### 4.3.1 Education

One key step toward finding solutions is for people to understand how these services are being funded, what kinds of information is being gathered about them, how their behavior is being manipulated, and the consequences of all this. A great deal of the rhetoric from the corporations using a surveillance capitalist business model has focused on individual choice, limitless access to information, empowerment, and personalization; but we view these as a hollow kind of choice and empowerment. Until recently there has been relatively little focus on the model's dark side of surveillance and manipulation. There have been flare-ups of negative reactions, for example, in 2004 to the initial description of how Google's Gmail scans private correspondence to place targeted advertising, but subsequently this became (perhaps grudgingly) accepted as normal. In the last few years, there has been a substantial shift as more of the extent of the surveillance and manipulation has become visible, especially in light of the reports of extensive online Russian targeting of the 2016 U.S. presidential election. In addition to numerous reports on election hacking, there have been increasing numbers of editorials, articles, and books on this topic, with Zuboff's book (2019) being an important milestone in terms of presenting the depth and broad scope of the problem along with an intellectual framing. Another noteworthy presentation is *The Social Dilemma*, a 2020 Netflix docudrama about the societal damage of social media.

It is essential that the education process continue, with ongoing discussion and exposure of the extent of surveillance and political and other behavior manipulation. It is also important that we do not fall into the trap of assuming such a world is now normal and acceptable. However, neither being in a state of numbness or grudging acceptance, nor being in a state of continual outrage for years, are attractive alternatives. We also need positive visions of how we can use information technology to support human flourishing without surveillance and manipulation, and the collective political will to move toward those visions.

#### 4.3.2 Resistance

There are several potential goals for resistance to surveillance capitalism, including personal integrity, undermining the profitability of this business model, and raising awareness and calling people to action. Trying to maintain personal integrity is of course important as an end in itself, and also in helping avoid having surveillance become normalized. However, such actions, or other actions whose purpose is to undermine the profitability of the business model, seem unlikely to have sufficient impact on their own. But doing these things (and discussing doing them and the challenges of doing them), can contribute to awareness and calls to action. Resistance can take a variety of forms. One is to simply not use certain parts of the IT infrastructure, e.g., the #DeleteFacebook movement. This certainly has merit, but can also make it difficult to participate fully in society, given the extent to which Facebook enters into many social interactions, into deliberations among members of a political movement, and so forth. It also recasts a political issue as a willpower issue (Giridharadas, 2019).

And it seems simpler to delete Facebook than for example Google, given Google's pervasiveness. As a more extreme example, Hill (2019) describes her attempt over a period of six weeks to block the five tech giants. Another important form is as art directed at the themes of surveillance and resistance (Zuboff, 2019, p. 491–492), which (among other things) can push back against such surveillance and manipulation as being considered normal.

Finally, there are various kinds of technical resistance that seek to avoid being tracked, or to disrupt surveillance. Regarding specific tools for such technical resistance, web browsers often provide a switch to block setting third-party cookies. This is only somewhat useful, since among other things it often just blocks cookie writing, not reading/sending. For example, if a user visits Facebook directly, it would be a first party and so a cookie could be set and then subsequently used by third parties. Also, there are many other techniques for tracking besides cookies, notably browser/machine fingerprinting (Nikiforakis et al., 2013). Web browsers may also provide a “do not track” setting — unfortunately, though, this option is effectively dead at present since it only works if trackers honor the request, and many do not. (But see the discussion of “do not

track” legislation in Section 4.1.) Simply turning off JavaScript can help as well, although doing so will also cause many sites to be unusable. There are also a variety of ad blocker plugins and other anti-tracking browser extensions, such as uBlock Origin<sup>1</sup>, Privacy Badger<sup>2</sup>, AdBlock Plus<sup>3</sup>, and Ghostery<sup>4</sup>. On the more stringent (and difficult-to-use) side, uMatrix<sup>5</sup> can be set up to block all third-party requests by default, and then let the user choose which domains to enable for a particular webpage. The Firefox browser itself also includes some tracking protection (Nguyen, 2018), including in “private browsing” mode. (In other browsers, “private browsing” modes may not really protect against tracking - the goal there is more to protect the user’s web history from someone with access to the user’s device.) Panopticklick<sup>6</sup> from the Electronic Frontier Foundation will analyze how well the user’s browser protects against tracking. A different approach is taken by Ad Nauseam<sup>7</sup>, built atop uBlock Origin, which simulates clicks on every blocked ad to generate a stream of meaningless data that obscures the user’s actual interests and behavior (also see (Howe & Nissenbaum, 2009)). Another is a Firefox add-on called Multi-Account Containers<sup>8</sup>, which are like normal tabs on a browser except that each container has its own preferences, advertising tracking data, and other information, which cannot be seen by the other containers, making it harder to do tracking across sites. (However, they can be unintuitive for users, and it can still be difficult for users to reason about tracking since webpages often load from so many different sources.) Relevant papers in the academic literature include an early study on tracking with measurements in Summer 2011 (Roesner, Kohno, & Wetherall, 2012), a longitudinal study of tracking 1996–present (Lerner, Simpson, Kohno, & Roesner, 2016), and a demonstration that anyone can buy ads to track a targeted individual (Vines et al., 2017).

Stepping back, one is struck by the considerable effort that is going into these technical approaches to resistance, how complex the solutions are, and the extent to which there is a cat-and-mouse game going on between the trackers and the tracked. The economic impact on surveillance capitalism of this technical resistance is liable to be limited by its complexity. However, the main practitioners of both its development and use, such as computer science students and software engineers, are also likely the potential employees of the big IT corporations, and employees are a scarce resource, so they may have power by other means (e.g., in 2018 Google dropped a contract with the Pentagon after an

---

1 <https://github.com/gorhill/uBlock>

2 <https://www.eff.org/privacybadger>

3 <https://adblockplus.org>

4 <https://www.ghostery.com>

5 <https://addons.mozilla.org/en-US/firefox/addon/umatrix/>

6 <https://panopticklick.eff.org>

7 <https://adnauseam.io>

8 <https://support.mozilla.org/en-US/kb/containers>

uprising of its employees (Harwell, 2018)). Finally, if technically skilled users find the landscape challenging and confusing, nontechnical users must find it even more so. If one were a journalist reporting from on-the-ground in a repressive regime, one can imagine it being reasonable to take these kinds of precautions. But should ordinary citizens who just don't want corporations tracking everything they do online need to do this also? Ultimately, the most important role for such technical resistance may be as part of education and helping build pressure for more comprehensive change.

## 4.4 Technology

As noted at the beginning of this section, in this endeavor, technology should not be taken as a given external force, but should instead be co-developed as needed, along with regulation and nudges toward new social practice. Fortunately, most of the technology needed to support alternatives to surveillance capitalism already exists — it is instead a matter of applying it. However, there are opportunities for additional work to support the regulatory work and possible societal shifts. In addition, the interoperability requirements proposed above would allow much more experimentation and exploration of novel technical approaches.

Here are key existing technologies for the program proposed here:

- open source
- APIs to support interoperability and portability
- encryption (e.g., for storing backups on a central server)
- peer-to-peer systems

For portions of the digital ecosystem that form the underlying digital commons in particular, *open source* means that the source code can be easily inspected, shared, and built upon by others.

APIs to support *interoperability and portability* are key to enabling a flourishing ecosystem of different applications that can function together, and that allow end users to move to different providers. At the infrastructure level, standard APIs support the notion of a commons, while at the application level, good APIs can support interoperability of such things as different social media systems (e.g., the ActivityPub standard). In general, interoperability counteracts overdependence on the part of users on service providers and reduces the possibilities of cutting off innovative competitors.

Another key technology is *encryption* to guard user privacy. It significantly helps address the problems that we summarized in Section 3.3 as the privacy dimension. We earlier discussed how Cloud Computing is a key enabling technology for surveillance capitalism. However, we do not go so far as to argue that everyone should keep all of their data on personal devices, backed up on



memory sticks kept in a shoebox in the closet. Centralized, reliable storage, with redundancy and good backups, can provide useful functionality without surveillance, if what is being sold is simply storage capacity, with everything encrypted (both what is stored and what is transmitted back and forth). With a separation between basic infrastructure, which can be rented analogous to “dark fiber” of internet service providers, and the content that is running on top of it, users reduce their dependence on their Cloud Computing provider without sacrificing the benefits or needing to become system administrators themselves. Overall, we want any technical solutions that are intended for general use to only require commonly available skills.

Finally, *peer-to-peer systems* may be an important tool for avoiding central control altogether in some situations. There are many platforms that label themselves as peer-to-peer, because peers do communicate with each other, but with the communication mediated via central servers of the platform provider. Such platforms are thus peer-to-peer only on a very superficial level. Instead, what we recommend here are peer-to-peer solutions on every level of the technical stack where power imbalances can become a problem. In particular, this implies that the communication channels be controlled by the peers. For such applications, the service provider has no way of stopping peers from using the application to communicate directly. This solves the problems we described as the first dimension in Section 3.3 technically. Instead of answering the question in whose hands power over the communication system might be relatively safe, they solve the problem of power by not letting it manifest in the first place. Note that this is a very strong requirement, and not every medium of communication needs to be decentralized on every level in this strong sense, nor may it be feasible. Nevertheless, we regard this as an effective pattern to be considered, particularly when there are significant imbalances of power and risks of coercion and control.

#### 4.4.1 Useful Technologies and Practices

On the services and application side, there are many examples of alternatives that address one or more of the issues raised earlier. For browsing, “Brave” is an open-source browser that (the company says) blocks ads and trackers, in both mobile and desktop versions. It includes a facility for giving micropayments to publishers using blockchain-based tokens. As an alternative search engine “DuckDuckGo” does not collect or share personal information. In addition, “Ecosia” donates 80% of its profits to NGOs that focus on reforestation, in order to mitigate the environmental impact of the industry. Both companies depend partially on other search engines such as “Bing” or “Yahoo!” and their business models are still based on advertising (and also affiliate marketing).

There is a variety of social media alternatives. “Mastodon,” “Matrix,” and “Diaspora\*” are all examples of donation-based social networks that use some

kind of federated server structure. Besides of course adoption and the network effect arising from Facebook's dominant position, for some of these architectures there are also problems with scalability. Furthermore, there is still a power imbalance between users and the federation. Federating these structures is a step in the right direction, but decentralization does not stop there. Some applications that go beyond federation and use truly peer-to-peer networks include "Junto," "Secure Scuttlebutt" (a self-hosted social media ecosystem), and "Aether" (which additionally introduces an election process for moderators of different communities and makes posts ephemeral). All of these have been designed from an awareness of problems of current social media, and all use some kind of peer-to-peer protocol in response. As a consequence, identity is not proven via passwords stored on a central sever, but by cryptographic signatures. This not only fulfills the minimum data requirement naturally but exceeds it in the way that there is no monolithic data accumulation and no central entity to monetize it. Differences exist in the data storage model. Whereas Secure Scuttlebutt uses the friendship graph to decide which data a peer stores, Aether is designed so that every peer can store all data, and Junto utilizes a Distributed Hashtable to distribute the storage space that the peer-to-peer network provides. In addition to the choice of where and what data is stored, an equally important design choice regards which content will get high exposure. In place of the Machine Learning supported algorithms that tech companies apply today and that are optimized for users maximizing time-on-site, other, different models and metrics are tried out. Interoperability helps to create an ecosystem in which users can choose the algorithms that work in their best interests, thus enabling an evolution that optimizes for these properties instead.

As a counter-design to corporate clouds, a variety of alternative models should be investigated. One important such example is the SOLID project<sup>1</sup> at MIT, headed by Tim Berners-Lee. In the context of alternatives to Cloud Computing, we propose that distributed ledger technology (DLT) play a key role in implementing truly peer-to-peer structures.

For this purpose we regard the most prominent DLT, classical blockchains, in this regard as insufficient, although we agree that decentralization is a key component in response to the data centric paradigm. Besides their issues with scalability and energy waste, on a blockchain all the data is held by every member and thus is still all in one place. The power would therefore only be distributed among everyone with the intelligence and algorithms to datamine it. Instead the decentralization needs to go far beyond the access of a data silo.

If these technologies are sufficiently easy to use, they can help bring about a shift in social practices. At the same time, the open source approach increases the formative influence that social movements have on the technology ecosystem. As mentioned, the emergence of technological alternatives depends on the regulatory

---

1 <https://solid.mit.edu/>

framework (and may even be funded partially through punitive damages). In particular, alternatives with ownership structures that transform semi-public spaces into common property are relevant in this context. However, technical tools can also be developed to help detect illegal behavior (under the regulatory regimes proposed here). These are just a few examples of how transformation in the three areas is mutually reinforcing.

## 4.5 Funding, Ownership, and Control

Under surveillance capitalism, much of our IT infrastructure, such as search, email, and social media, is funded by advertisers, with a small number of corporations owning and controlling the infrastructure. What happens if the business model of surveillance capitalism is undermined?

First let's consider ownership. Here it is appropriate to separate out different categories of things that might be owned:

- (1) Physical objects, including servers, buildings, networking equipment, fiber optic cables, and so forth (plus of course the end user devices such as laptops and mobile phones)
- (2) Software, including both system and application software
- (3) Data
- (4) Protocols and standards

Different considerations apply to these different categories. Physical objects will generally have a person, organization, or government who owns and maintains them.

For software, we suggested earlier (Section 4.4) that open source provides an important model, since then the source code can be easily inspected, shared, and built upon by others. In addition, it simply bypasses many of the issues around ownership. Open source projects still need contributors and governance structures, so the question of control remains but in a different and easier form. (If a group doesn't like the direction an open source project is going, they can just fork the code and make their own project.) The issues around data ownership are complex, as discussed earlier as well; and in many cases, it seems better not to gather (and retain) the data at all. Creative Commons and similar licenses are important tools for allowing photographs, written material, and much else to be shared and remixed, playing an analogous role to open source licenses for software. A caution here, however, is that licenses and practices that make sense for individuals and small organizations can be abused by massive data-gathering and surveillance capitalists (e.g., the use of millions of online photos for training facial recognition systems, or scenes from our streets and sidewalks that are part of the community fabric, but that also get appropriated by Google Streetview). Finally,

protocols and standards are good candidates for means such as open, participatory processes involving all the affected stakeholders and managed by publicly accountable bodies.

Of course, at present often a single large surveillance capitalist concern owns and controls all of these — but unbundling is liable to be part of strategies to curb their power. In addition, adversarial interoperability will allow experimentation with multiple models and evolution of approaches.

We now outline some alternatives for funding and controlling IT infrastructure.

#### 4.5.1 For-Profit Corporations

One option is for-profit corporations. We earlier (Section 4.1.3) suggested that the shift from context specific to targeted advertising marks the location of a suitable line to draw and challenge surveillance capitalism by prohibiting advertising based on personal profiling. However, for-profit corporations could continue to offer these services, supported by advertising, including context-specific advertising, just without personal profiling. Another funding option is fee-for-service. This option is thus still very much capitalism, just not surveillance capitalism.

There are existing corporations that use these models. Two systems to be noted in particular are Brave<sup>1</sup> and DuckDuckGo<sup>2</sup>. Brave is an open-source browser that (the company says) blocks ads and trackers, in both mobile and desktop versions. It includes a facility for giving micropayments to publishers of content being viewed using blockchain-based tokens. The DuckDuckGo search engine, according to the company, does not collect or share personal information. Its business model is still based on advertising (and also affiliate marketing). The ads shown on DuckDuckGo are based just on the keywords typed in the search box, rather than also on tracked personal information. Revenues come from Amazon and eBay affiliate programs: when users are referred to one of those sites by DuckDuckGo and then buy something, the company collects a commission.

Another idea here is to nudge the market by having institutions such as libraries, universities, and others buy ad-free, no tracking versions of services for their patrons/students, either from new companies, or from existing large IT corporations if they are willing to unbundle their services to support this. (Note that it would be essential to carefully monitor the corporations to ensure they are not tracking these users (Farivar, 2016; Peterson, 2015).)

#### 4.5.2 Public Funding and Public Control

Another alternative is public funding. As discussed in Section 3.3.4, this of course brings with it the danger of manipulation. However, there are a number of models for government funding of information that provide a guaranteed revenue stream

---

1 <https://brave.com>

2 <https://duckduckgo.com>

and insulation from immediate political pressures. One example is the public radio and television systems that exist in many countries, including Germany and the UK; another is the subsidies to newspapers that existed in the U.S. in the 19th century via subsidized postal rates and tax policy McChesney and Nichols (2010). Or there could be other programs that emphasize individual choice and responsibility. For example, “journalism vouchers” could be issued to every resident that would allow people to provide grants to investigative journalists, whose work would then appear on social media.

Earlier (Section 4.2) we suggested that content moderation was not a panacea for the problems of social media, but that some content moderation is necessary for the most extreme cases (e.g., live-streaming mass shootings). Who should have the power to decide that? For rapidly developing situations, this would likely be at the level of the network providers (either public or private), but overall policy for this should, we suggest, be set by democratically controlled and accountable public organizations, either at the national or international levels. There is no easy answer here; but the current situation, which leaves these questions ultimately to a few extremely wealthy individuals, seems wrong.

Related choices concern encryption software and crypto-currencies. Should there be trapdoors that allow duly authorized security forces to have access to encrypted contents? Here we would argue they should not: we simply disallow that power by technical means. (Again, this is not an issue with a completely simple answer and no tradeoffs — this choice means that actual terrorists would have access to secure encryption that shields them from intelligence services, as would everyone else.) Similarly, if crypto-currencies are set up to truly provide anonymity, there are obvious benefits; but they can also be used for example by criminals who have placed ransomware on hacked systems to get untraceable payments.

#### 4.5.3 NGOs and Cooperatives

Another possibility is having other societal institutions that control the service. If the continued existence of such institutions is insulated from day-to-day changes in public opinion, this removes one source of pressure to engage in propaganda or surveillance. One possibility here is NGOs (e.g., the Mozilla Foundation, which is the sole shareholder in the Mozilla Corporation). However, being a nongovernmental organization does not automatically guard against conflicts of interest arising from funding, nor does being an NGO automatically mean the organization will be benevolent. Minimally, a close look at the organizational structure is needed.

Scholz and Schneider (2017) advocate placing these alternatives in the hands of worker cooperatives. Using this model, more of the relevant stakeholders would be included in the ownership model, particularly if it also includes the end users of the infrastructure. However, if one takes a closer look at the ownership

structure, often the potential for conflicts of interest among different sub-groups of a coop becomes apparent. Although such a structure would be a significant advancement in the power balance, it still leaves open questions. By which mechanism would the formal owners coordinate and exercise their right to make decisions? What if one group of stakeholders, e.g., the programmers, refuse to implement the changes the majority of owners decided upon?

#### 4.5.4 No Funding or Minimal Funding

Freely contributed work is another alternative, at least for intangibles such as software and data. Examples such as Wikipedia and OpenStreetMap show how an enormous amount of knowledge can be contributed by volunteers, perhaps along with funding for hardware and support staff. Such a model can work well if a clear structure is provided that guides how to arrange and connect the different contributions.

#### 4.5.5 An Ecosystem Approach

We suggest that there are parts of the IT infrastructure which should be provided as a general commodity. The classification for which parts this is the case can change over time and therefore needs to be regularly object of public debate. Based on a decision that is grounded in democratic legitimation, regulatory and technological development can act in accordance. Against the background of the above problem analysis, we propose as essential decision criteria (1) the degree to which people depend on the services, (2) the relative monopoly position of the prevailing service providers, and (3) the business model of the service providers.

These criteria are helpful to decide which services should be provided as a general commodity. However, they tell us nothing about how this should be done. Considering the ‘how’, the different ownership structures offer varying degrees of protection against the discussed problems. The applicability of these structures to different parts of the services also varies. Therefore, we propose to go a multitude of ways that are interoperable with each other. For example, a service could run as open source software on a network that is hosted by small public institutions. These basic services would be free of charge and modules for additional functionality or UI could be provided by competing private companies.

Future work is required to paint a positive vision of a paradigm in IT that not only counters surveillance capitalism but also enhances the quality of life. This requires a change from the venture capital driven nature of the IT industry toward one that makes the development of IT more closely related to the real needs of society.

Our vision of a network of locally anchored software ecosystems based on decentralized software and data architectures could be called an ecosystem approach. Copyright scholar James Boyle has described how the term “ecology” marked a turning point in environmental activism. Prior to the adoption of this

term, people who wanted to preserve whale populations didn't necessarily see themselves as fighting the same battle as people who wanted to protect the ozone layer or fight freshwater pollution or beat back smog or acid rain. Similarly this ecosystem approach might mark a turning point for the IT industry and measures like adversarial interoperability would play a role in shaping the currently monopolistic landscape into a system, with higher diversity.

## 5 Conclusions

The direction in which the IT industry is moving is highly alarming. The business model of surveillance capitalism, left unchecked, poses an existential threat to liberal democracies, provides further tools for repression to autocratic regimes, and threatens the quality of life on this planet. We argued that this is a case of companies in monopoly positions playing their users' dependency against them. Therefore, True Informed Consent and Adversarial Interoperability, if implemented comprehensively, combat user exploitation and monopoly respectively. Overall, a new paradigm is needed in IT development that is no longer driven by the need to generate high profits through collecting large amounts of personal data and manipulating behavior, but is oriented to serve human needs while staying within planetary boundaries.

## 6 Acknowledgments

This research was funded by The University of Siegen through its graduate program “Supply Chains and Economic Development – Plural Perspectives” and the DFG SFB ‘Medien der Kooperation’ (Collaborative Research Centre ‘Media of Cooperation’).

## 7 References

- Allen, M. (2017, Nov 9). Sean Parker unloads on Facebook: “God only knows what it’s doing to our children’s brains”. Axios Newsletters. Retrieved from <https://www.axios.com/sean-parker-unloads-on-facebook-god-only-knows-what-its-doing-to-our-childrens-brains-1513306792-f855e7b4-4e99-4d60-8d51-2775559c2671.html>
- Avila, R., Freuler, J. O., & Fagan, C. (2018). The invisible curation of content: Facebook’s news feed and our information diets (Tech. Rep.). 1110 Vermont Ave NW, Suite 500 Washington, DC 20005, USA: World Wide Web Foundation. (<http://webfoundation.org/docs/2018/04/WF-InvisibleCurationContent-Screen-AW.pdf>)
- Bennett, L., Borning, A., Landwehr, M., Stockmann, D., & Wulf, V. (2020). Treating root causes, not symptoms: Regulating problems of surveillance and personal targeting in the information technology industries. G20 insights. Retrieved from <https://www.g20-insights.org/policybriefs/treating-root-causes-not-symptoms-regulating-problems-of-surveillance-and-personal-targeting-in-the-information-technology-industries/>
- Bradshaw, S., & Howard, P. (2017). Troops, trolls and troublemakers: A global inventory of organized social media manipulation (Vol. 2017.12; Tech. Rep.). Oxford, UK: Oxford Internet Institute. (<https://ora.ox.ac.uk/objects/uuid:cef7e8d9-27bf-4ea5-9fd6-855209b3e1f6>)
- Buettner, R. (2017, August). Predicting user behavior in electronic markets based on personality-mining in large online social networks. *Electronic Markets*, 27 (3), 247–265. Retrieved from <https://doi.org/10.1007/s12525-016-0228-z>
- Cadwalladr, C. (2018, Mar 18). The Cambridge Analytica files — ‘I made Steve Bannon’s psychological warfare tool’: Meet the data war whistleblower. *The Guardian*. Retrieved from <https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-facebook-nix-bannon-trump>
- Chen, Y., & Cheung, A. S. Y. (2017, June 26). The transparent self under big data profiling: Privacy and Chinese legislation on the social credit system. *The Journal of Comparative Law*, 12 (2), 356–378. (University of Hong Kong Faculty of Law Research Paper No. 2017/011. Available at SSRN: <https://ssrn.com/abstract=2992537> or <http://dx.doi.org/10.2139/ssrn.2992537>)
- Chin, J., & Wong, G. (2018, Nov 28). China’s new tool for social control: A credit rating for everything. *Wall Street Journal*. Retrieved from <https://www.wsj.com/articles/chinas-new-tool-for-social-control-a-credit-rating-for-everything-1480351590>
- Doctorow, C. (2020). How to destroy surveillance capitalism. *OneZero*. Retrieved from <https://onezero.medium.com/how-to-destroy-surveillance-capitalism-8135e6744d59>
- Duch-Brown, N., Martens, B., & Mueller-Langer, F. (2017, February). The economics of ownership, access and trade in digital data. JRC Digital Economy Working Paper 2017-01. (Available at SSRN: <https://ssrn.com/abstract=2914144> or <http://dx.doi.org/10.2139/ssrn.2914144>)
- Dufner, M., Arslan, R. C., & Denissen, J. J. (2018). The unconscious side of Facebook: Do online social network profiles leak cues to users’ implicit motive dispositions? *Motivation and Emotion*, 42 (1), 79–89.
- Farivar, C. (2016, Feb 3). Former, current students sue Google over university-issued Gmail scanning. *Ars Technica*. Retrieved from <https://arstechnica.com/tech-policy/2016/02/former-current-students-sue-google-over-university-issued-gmail-scanning/>



- Flick, C. (2016). Informed consent and the Facebook emotional manipulation study. *Research Ethics*, 12 (1), 14–28. Retrieved from <https://doi.org/10.1177/1747016115599568>
- Friedman, B., & Hendry, D. (2019). *Value sensitive design: Shaping technology with moral imagination*. Cambridge, Massachusetts: MIT Press.
- Friedman, B., Kahn, P. H., Jr., & Borning, A. (2006). Value Sensitive Design and information systems: Three case studies. In *Human-computer interaction and management information systems: Foundations*. Armonk, NY: M.E. Sharpe.
- Giridharadas, A. (2019, Jan 10). Deleting Facebook won't fix the problem. *New York Times*. Retrieved from <https://www.nytimes.com/2019/01/10/opinion/delete-facebook.html> (Op-ed)
- Hackenbroich, J., & Leonard, M. (2019, Aug 15). A fistful of dollars: Europe and US sanctions. *European Council of Foreign Relations*. Retrieved from [https://ecfr.eu/article/commentary\\_a\\_fistful\\_of\\_dollars\\_europe\\_and\\_us\\_sanctions/](https://ecfr.eu/article/commentary_a_fistful_of_dollars_europe_and_us_sanctions/)
- Harwell, D. (2018, June 1). Google to drop Pentagon AI contract after employee objections to the 'business of war'. *Washington Post*. Retrieved from <https://www.washingtonpost.com/news/the-switch/wp/2018/06/01/google-to-drop-pentagon-ai-contract-after-employees-called-it-the-business-of-war/>
- Hawley, J. (2019). Senate bill 1578: Do not track act. *Washington DC*. (<https://www.congress.gov/bill/116th-congress/senate-bill/1578/text>)
- Hill, K. (2019, February). Goodbye big five: Life without the tech giants. *Gizmodo*. (<https://gizmodo.com/tag/blocking-the-tech-giants>)
- Howe, D. C., & Nissenbaum, H. (2009). TrackMeNot: Resisting surveillance in web search. In I. Kerr, V. M. Steeves, & C. Lucock (Eds.), *Lessons from the identity trail: Anonymity, privacy, and identity in a networked society*. New York: Oxford University Press.
- Hummel, P., Braun, M., & Dabrock, P. (2020, June). Own data? ethical reflections on data ownership. *Philosophy & Technology*. Retrieved from <https://doi.org/10.1007/s13347-020-00404-9>
- Kaiser, A. J. (2018, Sep 26). The Brazilian group scanning WhatsApp for disinformation in run-up to elections. *The Guardian*. Retrieved from <https://www.theguardian.com/world/2018/sep/26/brazil-elections-comprova-project-misinformation-whatsapp>
- Keynes, J. M. (1971). The economic possibilities for our grandchildren. In *The collected writings of John Maynard Keynes*. Macmillan.
- Lenhart, A., & Owens, K. (2020, October). Good intentions bad inventions: The four myths of healthy tech. *Data and Society*. Retrieved from <https://datasociety.net/wp-content/uploads/2020/10/Healthy-Tech-Myths-DataSociety-20201007.pdf>
- Lerner, A., Simpson, A. K., Kohno, T., & Roesner, F. (2016). Internet Jones and the raiders of the lost trackers: An archaeological study of web tracking from 1996 to 2016. In *Proceedings of the 25th unix conference on security symposium* (pp. 997–1013). Berkeley, CA, USA: USENIX Association. Retrieved from <http://dl.acm.org/citation.cfm?id=3241094.3241172>
- Manokha, I. (2018). Surveillance: The DNA of platform capital – the case of Cambridge Analytica put into perspective. *Theory & Event*, 21 (4), 891–913. (Project MUSE, <https://muse.jhu.edu/article/707015/pdf>)
- Matz, S. C., Kosinski, M., Nave, G., & Stillwell, D. J. (2017). Psychological targeting as an effective approach to digital mass persuasion. *Proceedings of the National Academy of Sciences*, 114 (48), 12714–12719. Retrieved from <https://www.pnas.org/content/114/48/12714>
- McChesney, R., & Nichols, J. (2010). *The death and life of American journalism: The media revolution that will begin the world again*. Philadelphia, PA: Nation Books.

- Morozov, E. (2019, Feb 4). Capitalism's new clothes. The Baffler .  
(<https://thebaffler.com/latest/capitalisms-new-clothes-morozov>)
- Murphy, M. D. (2017, Dec 11). Transcript of excerpt from Chamath Palihapitiya's Stanford Biz School talk. Medium. Retrieved from <https://medium.com/@whileseated/transcript-of-excerpt-from-chamath-palihapitiyas-stanford-biz-school-talk-9856ed0beba9>
- National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research . (1978). The Belmont Report. Washington DC: United States Government Printing Office.
- Nguyen, N. (2018, Oct 23). Latest Firefox rolls out enhanced tracking protection. The Mozilla Blog. (<https://blog.mozilla.org/blog/2018/10/23/latest-firefox-rolls-out-enhanced-tracking-protection/>)
- Nikiforakis, N., Kapravelos, A., Joosen, W., Kruegel, C., Piessens, F., & Vigna, G. (2013). Cookieless monster: Exploring the ecosystem of web-based device fingerprinting. In Proceedings of the 2013 IEEE symposium on security and privacy (pp. 541–555). Washington, DC: IEEE Computer Society.
- Osoba, O. A., & Welser IV, W. (2017). An intelligence in our image: The risks of bias and errors in artificial intelligence. Rand Corporation.
- Peterson, A. (2015, Dec 28). Google is tracking students as it sells more products to schools, privacy advocates warn. Washington Post. Retrieved from <https://www.washingtonpost.com/news/the-switch/wp/2015/12/28/google-is-tracking-students-as-it-sells-more-products-to-schools-privacy-advocates-warn/>
- Pistor, K. (2020). The code of capital: How the law creates wealth and inequality. Princeton University Press.
- Richter, F. (2020, Aug 18). Worldwide market share of leading cloud infrastructure service providers. Statista. Retrieved from <https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers/>
- Roesner, F., Kohno, T., & Wetherall, D. (2012). Detecting and defending against third-party tracking on the web. In Proceedings of the 9th usenix conference on networked systems design and implementation (pp. 12–12). Berkeley, CA, USA: USENIX Association. Retrieved from <http://dl.acm.org/citation.cfm?id=2228298.2228315>
- Rohde, M., Aal, K., Misaki, K., Randall, D., Weibert, A., & Wulf, V. (2016). Out of Syria: Mobile media in use at the time of civil war. International Journal of Human-Computer Interaction, 32 (7), 515–531. Retrieved from <https://doi.org/10.1080/10447318.2016.1177300>
- Scholz, T. (2017). Überworked and underpaid: How workers are disrupting the digital economy. John Wiley & Sons.
- Scholz, T., & Schneider, N. (Eds.). (2017). Ours to hack and to own: The rise of platform cooperativism, a new vision for the future of work and a fairer internet. New York: OR Books.
- Sparks, D. (2020, Feb 6). Amazon's record 2019 in 7 metrics. The Motley Fool . Retrieved from <https://www.fool.com/investing/2020/02/06/amazons-record-2019-in-7-metrics.aspx>
- Swearingen, J. (2018, Oct 19). WhatsApp says it's too late to stop far-right fake news in Brazil. New York Magazine. Retrieved from <http://nymag.com/developing/2018/10/whatsapp-too-late-fake-news-brazil-election-bolsonaro.html>
- Talbot, D. (2014, July). Facebook's emotional manipulation study is just the latest effort to prod users. MIT Technology Review.
- Tufekci, Z. (2018, Mar 10). YouTube, the great radicalizer. New York Times. Retrieved from <https://www.nytimes.com/2018/03/10/opinion/sunday/youtube-politics-radical.html> (Opinion piece)

- Vengattil, M., & Dave, P. (2018, July 25). Facebook's grim forecast – privacy push will erode profits for years. Reuters Business News. Retrieved from <https://uk.reuters.com/article/uk-facebook-results/facebooks-grim-forecast-privacy-push-will-erode-profits-for-years-idUKKBN1KF2UA>
- Vines, P., Roesner, F., & Kohno, T. (2017). Exploring ADINT: Using ad targeting for surveillance on a budget - or - how Alice can buy ads to track Bob. In Proceedings of the 2017 on workshop on privacy in the electronic society (pp. 153–164). New York: ACM. Retrieved from <http://doi.acm.org/10.1145/3139550.3139567>
- Wulf, V., Misaki, K., Atam, M., Randall, D., & Rohde, M. (2013). 'On the ground' in Sidi Bouzid: Investigating social media use during the Tunisian revolution. In Proceedings of the 2013 conference on computer supported cooperative work (pp. 1409–1418). New York: ACM. Retrieved from <http://doi.acm.org/10.1145/2441776.2441935>
- Zinn, K. G. (2009, September). Satiation or two limits of growth: John maynard keynes. (Available at <https://www.indybay.org/newsitems/2009/09/01/18620369.php>)
- Zuboff, S. (2015, March). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, 30 (1), 75–89.
- Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. New York: PublicAffairs Books.