Problems with Surveillance Capitalism and Possible Alternatives for IT Infrastructure

Marvin Landwehr[a] Alan Borning[b], and Volker Wulf[a, c]

[a]School of Media and Information, University of Siegen, Siegen, Germany; [b]Paul G. Allen School of Computer Science & Engineering, University of Washington, Seattle, Washington, USA; [c]International Institute for Socio-Informatics (IISI), Bonn, Germany

ARTICLE HISTORY
Compiled December 8, 2021

ABSTRACT
Over the past two decades, the business model of surveillance capitalism has emerged in the IT industry. This model has turned out to be highly profitable, but, if left unchecked, will very likely undermine the foundations of liberal democracies and quality of life on this planet. It involve customized advertising and behavior manipulation, powered by intensive gathering and cross-correlation of personal information. There are significant indirect costs of this model, 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. Turning to what could be done, we propose a co-development of regulation and technology, as well as the key roles that can be played by citizens and civil society organizations. The regulatory measures are intended to safeguard privacy, require true informed consent, and to foster interoperability (even among rival firms, nonprofit organizations, and others). We also identify key enabling technologies, including open source, APIs to support interoperability and portability, encryption, and peer-to-peer systems. Finally, we discuss the crucial role of ownership structures for these IT services, and argue for an ecosystem approach as a counter narrative to surveillance capitalism.

KEYWORDS
Surveillance capitalism; political manipulation; economics; digital infrastructure; IT business models

Introduction

Over the past two decades, business models have emerged in the IT industries that have turned out to be highly profitable while providing services mostly free of charge for their end users. However, we argue that the economic successes of these business models that have radiated throughout the computing industry have moved it in a socially problematic direction.

In the following section we describe how the business models orient these companies toward amassing huge amounts of data about their users and toward centralization, as well as how their infrastructure innovations reflect and enhance these developments.

CONTACT Marvin Landwehr. Email: marvin.landwehr@student.uni-siegen.de

This article has been accepted for publication in *Information, Communication & Society*

We then situate the role of these business models in the conflict between growth imperatives and sustainability. Ultimately, they endanger liberal democracies, provide additional tools for surveillance and control to autocratic governments, and threaten the quality of life on this planet.

Next, we outline some possible solutions for these problems. This section is the core of the paper. We suggest a co-development of regulation and technology, along with key roles that can be played by citizens and civil society organizations, to challenge 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 actions in these areas interact with each other and show where they counteract the problem dimensions that we have identified. In particular, we propose regulatory measures that directly challenge the user surveillance and manipulation, and monopoly position of key corporate actors, that are central to the prevalent surveillance capitalism business model. We also identify key technologies to support this program, including open source, APIs to support interoperability and portability, encryption, and peer-to-peer systems. Finally, we discuss the crucial role of ownership structures for these IT services, and argue for an ecosystem approach as a counter narrative to surveillance capitalism.

Problematic Developments in the Computing Industry

In the aftermath of the dot-com-bubble, the surviving IT companies had to find business models that would continue providing a growing return to their venture capital funders. In order to keep increasing the user base, it was essential for free services to continue to be free of charge for the end users. Therefore it comes as no surprise that they chose to embed advertisements to generate revenue. However, the way in which they implemented this turned out to make them highly profitable at the expense of a devastating societal spillover. Instead of merely placing ads, user actions were tracked and recorded in large data bases. When computer scientists at these companies invented or refined algorithms to analyze effectively the giant volumes of data, and employed statistical methods (especially machine learning algorithms) to derive predictions from user profiles, the result was a new business model that turned out to be so profitable that even companies that were financed by fees also adopted this practice.

There are four phenomena taking place simultaneously. First, the companies are gathering enormous volumes of potentially relevant raw information by tracking the user, potentially including actions taken in the browser, contact addresses, mobile location, and more. Second, 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 can be 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 detailed 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 practice that is becoming increasingly relevant is the manipulation of user behavior on the basis of that data. A detailed knowledge of the environments to which a given user can be most usefully exposed to increase the probability of a desired behavior leads to a whole new category of customers. In addition to classical product advertisement, the companies can now offer political influence, particularly in general elections. 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.

Zuboff (2015, 2019) has named this business model "surveillance capitalism," and we use this same term here as well — and agree that this is a model with far-reaching and highly negative consequences. The problems of surveillance capitalism are not simply issues of surveillance and loss of privacy. Rather, it is in addition an attempt at a radical and ominous automated manipulation of behavior that is undermining sustainability, democracy, human dignity, and much more.

We adopt Zuboff's definition of surveillance capitalism, with two modifications. First, we want to extend the definition to include corporations whose business centers on selling goods and services to end users, as well as on corporations offering services at no cost to them. The key elements that differentiate these businesses from others are the intensive collection of personal data, in particular the "data exhaust" of additional information produced as a by-product of the user's primary activity, tracking and cross-correlation between multiple contexts, and attempted behavioral manipulation based on this data. Second, we take an interactional stance on the question of the degree to which people can be manipulated by social media and other services, in analogy with the interactional stance taken by value sensitive design (Friedman & Hendry, 2019; Friedman, Kahn, & Borning, 2006) regarding technology and human values. Thus, 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 certainly not neutral either.

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.

The Technological Infrastructure

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. 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 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 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 adver-

tisement 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?

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 rank, 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.

The trends in the computing industry of cloud computing and machine learning are therefore intertwined with the large IT companies' orientation towards surveilling their users and commercializing the resulting software and infrastructures. Language recognition is an example that demonstrates how the functionality developed in support of the business model evolves and feeds 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.)

We therefore categorize cloud computing and recent forms of machine learning as enabling technologies that in part emerged from and that feed into surveillance capitalism. 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. It is worth looking not only at how this infrastructure is used to generate revenue streams, but also at the selective denial of its use to exercise power.

Problems for Democracy and Sustainability

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. While the 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.

For a more detailed discussion of this influence, we refer to other sources (Doc-

torow, 2020; Landwehr, Borning, & Wulf, 2019; Zuboff, 2019). In summary, the current business models have a specific effect on the orientation of these IT companies; in particular, they lead to intensive gathering, tracking, and correlation of personal data. Problematic outcomes are encouraging rampant consumerism (which is incompatible with living sustainably on the earth), and behavioral manipulation targeted at individuals that undermines any democratic system.

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., attempted manipulation of political convictions) on a larger scale and with fine-grained targeting based on detailed knowledge of individuals. The question is therefore what to do about these powerful tools and the way they are used.

Despite the very dark sides of surveillance capitalism, at the same time these services 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 paradigms 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.

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. Regulation will be a key element of a response. However, regulation should not simply be a reaction to technology and an attempt to curb its worst excesses: technology should not be taken as a fixed, external force that will inevitably follow a particular path. Nor is surveillance capitalism at its root a technological problem amenable to a purely technological fix. Instead, regulation and technology should be co-designed and co-evolved. Citizens and civil society organizations will play key roles as well, by pushing for more effective regulation and supporting technologies, by helping to foster alternative models for providing needed services, and by adopting new social practice.

Regulation and Law

Regulation and law form key elements of possible solutions. We suggest four principal goals for regulation: protecting privacy, erecting barriers to behavior manipulation, protecting free speech and civic participation, and (probably most controversially)

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.

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. However, 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. 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 while browsing websites and potentially while using other internet-based services.

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, but not 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) the concept of "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.

Adversarial Interoperability

The current IT landscape is dominated by a very small number of companies in monopoly positions. Breaking up monopolies would be a useful step in ensuring that users are not too dependent on a single service provider. However, in our view, simply splitting Facebook, for example, into 6 mini-Facebooks, each with the same surveillance capitalism business model, would not be a particularly effective approach. Better would be 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 a monopoly in its niche, so a comprehensive approach must go further. And given the network effect and the resulting centralization mentioned above, which are 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 or to serve specialized markets. In his recent book *How to Destroy Surveillance Capitalism*, Doctorow (2020) uses the term "adversarial interoperability" (or "competitive compatibility" (Doctorow, 2021)), capturing that interoperability cannot be expected to be implemented voluntarily by for-profit companies if doing so might reduce their profits. But having such interoperability would make it easier for for-profit competitors to enter the market, as well as nonprofit or public entities, and therefore should be legally enforced. Doctorow (2020) 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 to it. Otherwise, Facebook, for example, could use intellectual property law to prevent users from scraping their own content and uploading it onto competing systems. The same is true for cloud computing providers. Therefore, IP restrictions are quite consequential and must be considered 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. Furthermore, 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.

Consequences for the Business Models

The regulations we suggest would significantly challenge the surveillance capitalism business model and help to foster alternatives. Let us therefore consider which business models would still be possible under such regulatory regimes.

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. 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, even if advertising were to be dropped completely, control over the infrastructure could still be used for attempted behavioral manipulation, and for censorship or selective denial of service (e.g., AWS withdrawing support for Parler), with all the resulting political problems. 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).

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.

The Role of Content Moderation

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.

Property Rights for Private Data

Finally, we want to make note of the approach of modeling 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. We view this approach as problematic. 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 for democracy and sustainability would be addressed by this approach.

More generally, current legal frameworks seem incompatible with the very idea of data ownership (Hummel, Braun, & Dabrock, 2020). 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? The inevitable legal inadequacies (Zech, 2012, p. 117–119), 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.

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 support for new social practice. Fortunately, technology that can support good alternatives to surveillance capitalism already exists — it is instead a matter of adopting and applying it. However, there are many opportunities for additional research and software development to support the regulatory work and possible societal shifts, and perhaps to develop even better alternatives. In addition, the interoperability requirements proposed in the section on adversarial interoperability 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 adversarial 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 adversarial 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. We earlier mentioned that 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 that can be rented (analogous to "dark fiber" of internet service providers), and the applications and content that use this infrastructure, users reduce their dependence on their cloud computing providers 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 can 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 consider here are comprehensive peer-to-peer systems, which mean that the service provider has no way of stopping peers from using the application to communicate directly. Note that this is a very strong requirement, and not every medium of communication needs to be decentralized to this extent, nor may it be feasible. Nevertheless, this as an effective pattern, particularly when there are significant imbalances of power and risks of coercion, censorship, or control.

For social media, 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 scaleability. 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 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. Another important design choice concerns 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 being tried. Interoperability helps to create an ecosystem in which users can choose and experiment with the algorithms that work in their best interests.

As a counter-design to corporate clouds, a variety of alternative models should be investigated. One important such example is the SOLID project [1] 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.

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 can have on the technology ecosystem. As mentioned, the emergence of technological alternatives depends on the regulatory framework (and may even be funded partially through punitive damages). 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 transformations in technology and law are mutually reinforcing.

Suggestions for Citizens and Civil Society Organizations

We have suggested that regulation should be co-designed and co-evolved along with the technology. In this section, we go on to make some suggestions for citizens and civil society organizations that may help marshal support for more effective regulation, counter some of the excesses of the current business model, and foster alternative models for providing needed services. Social practice can of course not be designed and imposed in the same way that regulations can be. 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.

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 hollow kinds of choice and empowerment.

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

[1] https://solid.mit.edu/

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.

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. 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, however, 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.

Finally, there are various kinds of technical resistance that seek to avoid being tracked, or to disrupt surveillance. These include such tools as ad blocker plugins and other anti-tracking browser extensions, sites that analyze how well a a user's browser protects against tracking, and even a tool that simulates clicks on every blocked ad to generate a stream of meaningless data that obscures the user's actual interests and behavior. See our earlier paper (Landwehr et al., 2019) for technical details.

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. Ultimately, the most important role for such technical resistance may be as part of education and helping build pressure for more comprehensive change.

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 us consider ownership. Here it is appropriate to separate out different categories of things that might be owned:

(1) Physical infrastructure, 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 infrastructure will generally have a person, organization, or government who owns and maintains them. For software, 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. The issues around data ownership are complex, as discussed earlier as well; and in many cases, it seems better not to gather or retain the data at all. Finally, protocols and standards are good candidates for governing structures 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 likely to be one 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.

For-Profit Corporations

One option is for-profit corporations. We earlier 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. These options are 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[2] and DuckDuckGo[3]. Brave is an open-source browser that (the company says) blocks ads and trackers, in both mobile and desktop versions. 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).

Another option 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 monitor the corporations carefully to ensure they are not tracking these users (Farivar, 2016; Peterson, 2015).)

Public Funding and Public Control

Another alternative is public funding. This of course brings with it the danger of manipulation by the state. However, there are a number of models for government funding of information that provide a guaranteed revenue stream 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 & 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 and other outlets.

Related choices concern encryption software and crypto-currencies. Should there be trapdoors that allow duly authorized security forces to have access to encrypted

[2] `https://brave.com`

[3] `https://duckduckgo.com`

contents? Here we would argue they should not: we simply disallow that power by technical means. (Again, this is not an issue with an obvious 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 cryptocurrencies 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.

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. 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.

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.

An Ecosystem Approach

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, including a cultural shift; IT professionals should rethink their role as enablers of societal opportunities.

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. Similarly this ecosystem approach might mark a turning point for the IT industry, and requirements such as adversarial interoperability could play a role in shaping the currently monopolistic landscape into a system with higher diversity.

Conclusion

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 to a considerable degree a case of companies in monopoly positions playing their users' dependency against them. True informed consent and adversarial interoperability, if implemented and enforced comprehensively, combat user exploitation and monopoly respectively. These regulations must be accompanied by technological development and innovation, along with pressure from citizens and civil society organizations. Our hope is that this will then allow society to move away from reliance on surveillance capitalism to provide basic IT services, and allow alternative models would emerge. 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.

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"). We also want to thank the School of Media and Information for its infrastructure support.

References

Doctorow, C. (2020). *How to destroy surveillance capitalism.* OneZero. Retrieved from `https://onezero.medium.com/how-to-destroy-surveillance-capitalism-8135e6744d59`

Doctorow, C. (2021, September). Competitive compatibility: Let's fix the internet, not the tech giants. *Communications of the ACM*, *64*(10), 26–29.

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/`

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)

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`

Landwehr, M., Borning, A., & Wulf, V. (2019). The high cost of free services: Problems with surveillance capitalism and possible alternatives for it infrastructure. In *Proceedings of the 2019 workshop on computing within limits.* New York: ACM.

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`)

National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. (1978). *The Belmont Report.* Washington DC: United States Government Printing Office.

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.

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.

Zech, H. (2012). *Information als schutzgegenstand.* Tübingen, Germany: Mohr Siebeck. Retrieved from `https://library.oapen.org/handle/20.500.12657/43908`

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.