



# In Defense of ‘Surveillance Capitalism’

Peter Königs<sup>1</sup> 

Received: 10 April 2024 / Accepted: 23 August 2024 / Published online: 16 October 2024  
© The Author(s) 2024

## Abstract

Critics of Big Tech often describe ‘surveillance capitalism’ in grim terms, blaming it for all kinds of political and social ills. This article counters this pessimistic narrative, offering a more favorable take on companies like Google, YouTube, and Twitter/X. It argues that the downsides of surveillance capitalism are overstated, while the benefits are largely overlooked. Specifically, the article examines six critical areas: i) targeted advertising, ii) the influence of surveillance capitalism on politics, iii) its impact on mental health, iv) its connection with government surveillance, v) its effects on the rule of law and social trust, and vi) privacy concerns. For each area, it will be argued that concerns about surveillance capitalism are unfounded or exaggerated. The article also explores some benefits of the services provided by these technology companies and concludes with a discussion of the practical implications. Throughout, the article draws on empirical evidence relating to the societal and political impact of digital technologies.

**Keywords** Big Tech · Surveillance · Privacy · Democracy · Social media · Big data · Mental health

---

✉ Peter Königs  
peter.koenigs@tu-dortmund.de

<sup>1</sup> TU Dortmund, Institut für Philosophie und Politikwissenschaft, Emil-Figge-Straße 50, 44227 Dortmund, Germany

## 1 Introduction

Critics of data-collecting tech giants such as Google, YouTube and Twitter/X have painted an alarming picture of what they call ‘surveillance capitalism’. Comparing these companies to brutal conquistadors or blood-smelling predators, critics blame surveillance capitalism for all kinds of social and political ills and mark it as one of the great evils of our time.<sup>1</sup> My project in this paper is to challenge this pessimistic narrative and to offer a more positive perspective.

Like many developments associated with the rise of information technology and artificial intelligence, surveillance capitalism is a complex and morally ambivalent phenomenon. I am not going to deny that there are risks and downsides associated with surveillance capitalism. However, the extremely pessimistic and at times alarmist perspectives on the topic, prevailing in both scholarly and popular discourse, are in my view misguided. Many critical discussions of surveillance capitalism suffer from two defects. They often exaggerate the negative aspects of surveillance capitalism, and they fail to acknowledge its positive aspects. The picture that emerges after correcting these biases will not be uniformly rosy, and this paper seeks to do justice to the ambivalence of the issue. But the emerging picture will be a lot more positive than critics would have us believe.<sup>2</sup>

I start by clarifying what I mean by surveillance capitalism and why I find the term itself problematic (Sect. 2). In the subsequent sections, I address six major concerns raised by critics, attempting to explain why their worries about these issues may be exaggerated. I discuss targeted online advertising (Sect. 3), the political impact of surveillance capitalism (Sect. 4), its impact on mental health (Sect. 5), its relationship with government surveillance (Sect. 6), its effects on the rule of law and social trust (Sect. 7), and privacy implications (Sect. 8). I then say a bit more about the positive aspects of surveillance capitalism (Sect. 9). I conclude by reflecting on the broader significance of the findings (Sect. 10).

My discussion of potential problems with surveillance capitalism is inevitably selective. The critical literature surrounding Big Tech is large, and I cannot here do justice to all of it. This article is organized around a selection of six key concerns that strike me as important and that are recurrent in academic and popular debates. Shoshana Zuboff, the most prominent critic of surveillance capitalism, will serve as one key reference point among others.

<sup>1</sup> The comparisons are due to Zuboff (2019, pp. 141, 192) and Véliz (2020, p. 25). Zuboff’s use of such terms as ‘chaos and terror,’ (2015, p. 81) ‘atrocities,’ ‘poison,’ (2022, pp. 7, 34), ‘parasitic,’ ‘vampire,’ ‘kidnapping,’ ‘violent battle,’ and even ‘final solution’ (2019, pp. 128, 192, 9) to describe surveillance capitalism falls within the same rhetorical category. Zuboff and Véliz are among the most vocal critics of surveillance capitalism. Other critical literature that this article engages with is referenced in the relevant sections throughout.

<sup>2</sup> Some of the few authors who have questioned the pessimistic narrative, anticipating many of the points made in this essay, include economists Bryan Caplan (2019) and Tyler Cowen (2019, ch. 6), journalist Robby Soave (2021), historian of ideas Johan Norberg (2023, ch. 5), and science and technology scholar Lee Vinsel (2021).

This paper, though primarily philosophical, will draw extensively on empirical literature. The seriousness of many concerns relating to surveillance capitalism depend on empirical facts, which philosophical discussions need to engage with. In some areas, the empirical literature is extensive, such as on echo chambers, filter bubbles, polarization, and mental health issues. Here, particular attention will be given to studies that offer a summary overview of existing research (review studies, meta-analyses, umbrella reviews). In other areas, such as whether algorithms exhibit political bias, the empirical literature is still scarce, and we must do without review studies. Limitations, ambiguities or contradictions within the empirical literature will be highlighted throughout.

## 2 On 'Surveillance Capitalism'

Surveillance capitalism relates to the practice of internet companies of offering typically free-of-charge online services and generating revenue by monetizing user data, especially through targeted advertising. The term, popularized by Zuboff and embraced by many others, seems to be a bit of a misnomer.<sup>3</sup> Both the 'surveillance' part and the 'capitalism' part in 'surveillance capitalism' are misleading.

Consider first 'surveillance'. Some scholars have proposed definitions of 'surveillance' according to which the practices of surveillance capitalism companies (henceforth 'SC companies') qualify as surveillance. Macnish, for instance, defines surveillance "as simply the sustained monitoring of a person or people", irrespective of the purpose of the monitoring.<sup>4</sup> A narrower definition has been offered by Lyon, who defines as surveillance "any collection and processing of personal data, whether identifiable or not, for the purposes of influencing or managing those whose data have been garnered."<sup>5</sup> On these accounts, the practices of SC companies qualify as genuine cases of surveillance. However, the case could be made that these and similar definitions miss an important aspect. We usually do not speak of surveillance unless the monitoring or data-collecting serves the purpose of verifying that people comply with certain normative expectations, such as laws, moral norms, orders, etc.

For instance, contrary to Macnish's definition, I do not believe we would classify a football coach's scouting of a potential transfer target as 'surveillance', although it involves 'sustained monitoring'. Similarly, contrary to Lyon's definition, it feels unnatural to categorize as 'surveillance' a coaching staff's collecting and processing of performance data of their players to improve their game, although this serves to 'influence or manage those whose data have been garnered'. This seems more like mere monitoring or observing than surveillance. In contrast, we may refer to it as surveillance when the coaching team keeps tabs on its players to ensure they eat

<sup>3</sup> Talk of 'surveillance' or 'surveillance capitalism' in this context is common in the literature (see e.g. Benn & Lazar, 2022; Risse, 2023, ch. 8; Vaidhyanathan, 2018; Véliz, 2020; Venkatesh, 2021; Williams & Raekstad, 2022).

<sup>4</sup> Macnish, 2018a, p. 10.

<sup>5</sup> Lyon, 2001, p. 2.

healthily and refrain from partying before match days, imposing penalties on those who do not comply. Surveillance, it seems, is about ensuring that individuals comply with certain normative expectations.

This perspective on surveillance aligns with definitions that highlight the prevention of crime or wrongdoing as its primary objective. MacQuade and Danielson, for instance, suggest that.

[m]onitoring is a general term that refers to the systematic, continual, and active or passive observation of persons, places, things, or processes. By contrast *surveillance* is used to indicate targeted monitoring of activities by police or security officials for specific evidence of crimes or other wrongdoing. Surveillance focuses on individuals, buildings and properties, or vehicles deemed suspicious on the basis of credible information that they are connected in some way to illegal or otherwise inappropriate activity.<sup>6</sup>

Similarly, the Cambridge Dictionary defines surveillance as “the careful watching of a person or place, especially by the police or army, because of a crime that has happened or is expected.”<sup>7</sup> While I do not think that the agents of surveillance are limited to the police, security officials, or the army, the above definitions capture what appears to be an important aspect of surveillance, namely that it is about tracking and preventing ‘inappropriate activity’.

If we understand surveillance as being about ensuring that people comply with certain normative expectations, then surveillance capitalism typically does not involve any surveillance. With one exception to which I shall return, SC companies are typically not in the business of ensuring that people comply with normative expectations. Their primary aim in collecting and processing user data is monetizing these data, not enforcing norms. Targeted advertising, arguably the core business of surveillance capitalism, seeks to nudge people towards purchases, not to police them.

I do not want to dismiss alternative definitions, such as those by Macnish or Lyon, as they may have their uses. The exact meanings of everyday terms like ‘surveillance’ are not always clear-cut, and one is free to define them according to one’s needs. Also, the substantial questions are rarely affected by terminological choices. However, because of the unfitting associations with policing that the term ‘surveillance’ evokes, I believe it is misleading in this context.

The ‘capitalism’ part in surveillance capitalism is also confusing and ill-specified. To frame the problem in Aristotelian terms: The *differentia specifica* is relatively clear – the defining feature of surveillance capitalism is that it involves the collection and use of data. But the *genus proximum* is poorly specified. It is unclear what *kind of thing* we are talking about. On a dedicated definition page in her book, Zuboff offers as many as eight different definitions. She characterizes surveillance capitalism as (1) an economic order, (2) an economic logic, (3) a ‘mutation’ of capitalism, (4) a foundational economic framework, (5) a threat, (6) the origin of a type

<sup>6</sup> McQuade III & Danielson, 2005, p. 1228.

<sup>7</sup> Cambridge Dictionary.

of power, (7) a movement, and (8) an expropriation of human rights.<sup>8</sup> Elsewhere, she characterizes surveillance capitalism as a 'market form' or a 'business model'.<sup>9</sup> These are all different kinds of things, or *genera proxima*. What kind of thing, then, is surveillance capitalism supposed to be?

Attempting to bring order to the varied usages, it appears that the term is primarily used to refer to either:

the business practices of tech companies like Google, YouTube and Facebook insofar as they generate revenue by collecting and monetizing user data (e.g., through targeted advertising), typically in exchange for free-of-charge online services.

or.

a capitalist economic system that is characterized by the domination of these business practices, or, in Zuboff's terms, a system where these business practices have become 'the dominant logic of accumulation'.<sup>10</sup>

I prefer the first usage. My reasons for this are twofold. First, critics of surveillance capitalism seem to be objecting to these business practices irrespective of whether they are becoming the 'dominant logic of accumulation' or not. Second, it is unclear whether these business practices really are becoming the 'dominant logic of accumulation', as Zuboff believes. The exact size of the current SC economy, let alone its future trajectory, is difficult to gauge. But to offer some perspective, the entire digital advertising market in the US is projected to reach 298 billion US dollars in 2024.<sup>11</sup> In contrast, the revenue of the US's single largest company by revenue, Walmart, stands at 648 billion US dollars.<sup>12</sup> In terms of market capitalization, the two most important SC companies, Alphabet (Google, YouTube) and Meta (Facebook, Instagram, WhatsApp), rank 4th and 6th, respectively.<sup>13</sup> At the time of Musk's takeover, Twitter/X with a market capitalization of some \$38 billion was not even among the top 100 US companies.<sup>14</sup> Topping the list are two tech giants, Microsoft and Apple, that earn their revenue primarily from other sources, such as hardware, software, server products, cloud computing, and gaming.<sup>15</sup> The second usage of the term, which insinuates the dawn of an entirely new type of capitalism dominated by SC business practices, therefore seems misleading.

<sup>8</sup> Zuboff, 2019, p. ix.

<sup>9</sup> Zuboff, 2015, passim; 2019, passim.

<sup>10</sup> Zuboff, 2019, p. 14.

<sup>11</sup> As of April 2024 (Digital Advertising – United States).

<sup>12</sup> As of April 2024 (Fortune 500: Walmart).

<sup>13</sup> As of April 2024 (Biggest Companies by Market Cap).

<sup>14</sup> Largest Companies by Market Cap. Now privately owned, Twitter/X typically no longer appears in rankings of companies by market capitalization.

<sup>15</sup> Note that not all companies that make up 'Big Tech' are SC companies in the narrow sense used here. The scope of this paper is thus fairly narrow and differs from that of more sweeping critiques of the tech industry, such as Morozov's critique of the techno-solutionist mindset (2013) or Srnicek's critique of 'platform capitalism' (2017).

For these reasons, I shall use the term ‘surveillance capitalism’ in the first of the two ways. This usage captures the critical discourse surrounding the term. Opponents of surveillance capitalism are criticizing what SC companies are doing – whether it is the ‘dominant logic of accumulation’ or not. Here, I offer a cautious defense of what these companies are doing.

It is possible that the nefarious-sounding term ‘surveillance capitalism’ was chosen more for its rhetorical effect than its semantic adequacy. Given its widespread use in the debate, I will also use it in this paper. But I wish to register my reservations.

### 3 Surveillance Capitalism and Targeted Advertising

The placement of online targeted advertisements is at the heart of surveillance capitalism. The main reason SC companies gather vast amounts of user data is to generate revenue by charging advertisers for placing targeted ads.<sup>16</sup> The fact that users are exposed to this type of advertising – also known as personalized or behavioral advertising – is among the most common complaints about surveillance capitalism.<sup>17</sup>

At first glance, it is not evident why targeted advertising should be a major concern. Being exposed to ads for products that match one’s interests is on the face of it unproblematic. Admittedly, targeted advertising can be annoying. A browsing experience without targeted ads would certainly be more enjoyable. However, the inconvenience caused by targeted advertising seems relatively minor. Moreover, this nuisance is not unique to *targeted* ads. Traditional advertising, which often presents ads for products of no interest to the viewer, could be considered even more bothersome.<sup>18</sup>

However, some suggest that there exists a deeper, more fundamental issue with targeted advertising. The core concern, as some argue, is that targeted ads are inherently manipulative. While conventional advertising can be manipulative too, targeted advertising, which leverages detailed information about individual users, is markedly more so. This exacerbates the pre-existing concern about advertising’s manipulative nature. And such manipulation is concerning because it compromises personal autonomy. Thus, according to this critique, one principal problem with surveillance capitalism is that it erodes personal autonomy by subjecting individuals to highly manipulative targeted advertising.<sup>19</sup>

There are three reasons why a critique of surveillance capitalism along these lines has limited force. First, any act of manipulation and the associated reduction in autonomy can vary in moral seriousness. Targeted advertising is arguably on the ‘not so serious’ end of the spectrum. As Benn and Lazar note, the seriousness of

<sup>16</sup> Revenues from advertising account for some 98% of Meta’s revenue (Johnston 2023).

<sup>17</sup> E.g. Calo, 2013; Spencer, 2020; Susser, Roessler, & Nissenbaum, 2019a, 2019b; Véliz, 2020; Zuboff, 2019.

<sup>18</sup> Similarly, Soave, 2021, pp. 121–122.

<sup>19</sup> Susser et al., 2019a, 2019b.

a given instance of manipulation depends on its efficacy and on what is at stake, and targeted advertising appears neither extraordinarily effective nor does it carry particularly high stakes.<sup>20</sup> Surprisingly, existing research on targeted advertising offers a mixed picture of its effectiveness. Some studies confirm its superior effectiveness.<sup>21</sup> Others yield more ambiguous results, indicating that its effectiveness is highly variable and might even be negative due to privacy concerns or perceived 'creepiness'.<sup>22</sup> A review paper summarizing existing research concludes that "[o]verall, the findings are much more nuanced than the industry's promise that [targeted advertising] boosts ad effects."<sup>23</sup> Another study reviewing the state of research notes that "[a]lthough, personalized advertising has become a prevalent marketing strategy, and many practitioners believe that personalized advertising is more effective than generic advertising, scholars have reported somewhat mixed results regarding how different levels of personalization affect consumer reactions".<sup>24</sup> Despite some remaining uncertainty, the evidence does not seem to support the popular notion that online targeted advertising has reached an entirely new level of manipulation, turning users into mind-controlled zombies. Regarding what is at stake, a successful targeted ad might lead a person to purchase a product they actually find useful. Undoubtedly, there are instances where targeted advertising might lead people to spend on products they do not need. However, there are worse things than encouraging people to purchase products that align with their interests. I am not disputing that there is something questionable about how targeted advertising tries to influence purchasing decisions. But when compared to other more serious autonomy-reducing manipulations the manipulation in targeted online advertising does not seem too alarming.<sup>25</sup> Susser et al.'s description of targeted advertising as a "grave threat" and "insidious" appears exaggerated.<sup>26</sup>

Second, when assessing the impact of surveillance capitalism on consumers' autonomy, we must consider the numerous ways in which the services provided by SC companies *enhance* consumer autonomy and diminish their vulnerability to manipulation in the marketplace. Susser et al. refer to Joseph Raz's account of autonomy.<sup>27</sup> "The ideal of personal autonomy", Raz writes, "is the vision of people controlling, to some degree, their own destiny, fashioning it through successive decisions throughout their lives."<sup>28</sup> Autonomy is compromised, for instance, when one is "forced by circumstances, or deceived by one's own ignorance, or governed by one's

<sup>20</sup> Benn & Lazar, 2022, pp. 140–141; see also Véliz, 2020, p. 146.

<sup>21</sup> De Kezer et al., 2022a; Guo & Jiang, Tran et al., 2020.

<sup>22</sup> E.g. Aguirre, Mahr, Grewal, de Ruyter, & Wetzels, 2015; Bang et al., 2019; De Keyser et al., 2022b; Kim et al., 2022; Lambrecht & Tucker, 2013; Winter et al., 2021.

<sup>23</sup> Boerman, Kruikemeier, & Zuiderveen Borgesius, 2017, p. 369.

<sup>24</sup> Bang et al., 2019, p. 1118. Two further summaries of the literature also paint rather mixed pictures (Boerman & Smit, 2023, p. 63; Varnali, 2019; pp. 9–10).

<sup>25</sup> Similarly, Benn & Lazar 2022, p. 141.

<sup>26</sup> Susser et al., 2019b, pp. 9, 13.

<sup>27</sup> Raz, 1988.

<sup>28</sup> Raz, 1988, p. 156.

weaknesses.”<sup>29</sup> On this account, targeted advertising, aiming at subverting people’s control over their purchasing decisions, diminishes autonomy. However, this same account of autonomy also seems to imply that the benefits provided by SC companies greatly compensate for such reductions. For example, consider a few of the services offered by Google. Its search engine equips users with immediate access to a vast range of information about almost anything, including potential purchases. Google also provides user reviews for nearly every product and service available, along with reviews of stores, businesses, and other entities. Product review videos are available on YouTube (which is owned by Google). Such services, merely a fraction of those provided by SC companies, empower consumers and boost their autonomy. If, as Raz contends, ignorance, deception, and manipulation weaken autonomy, then having comprehensive, trustworthy information readily accessible literally at one’s fingertips must surely enhance it. With the advent of surveillance capitalism, it has become unprecedentedly easy for consumers to resist deception and manipulation in the marketplace, enabling them to make informed and rational purchasing choices. One characteristic feature of surveillance capitalism, online targeted advertising, might slightly curtail consumer autonomy. But thanks to the services users get in return, the net effect on consumers’ autonomy is probably favorable by a large margin.

Finally, users who want to avoid targeted advertising can take various simple steps to reduce their exposure. These include disabling cookies, browsing in incognito mode, and using services (e.g. search engines) that do not collect user data and/or do not display any ads. Several service providers (including Google, YouTube, and Twitter/X) also allow users to opt out of targeted advertising for free,<sup>30</sup> and some (including Facebook, Instagram, Yahoo and YouTube) offer the option to opt out of advertising all together for a fee.<sup>31</sup> Another way to reduce exposure to both targeted and non-targeted ads is the use of ad-blocking software, although its effectiveness varies.<sup>32</sup> For those wary of being manipulated into making irrational purchases, having a policy of not clicking on ads goes a long way toward preventing such purchases. There thus exist numerous easy and effective methods for individuals to reduce, if not completely eliminate, exposure to targeted advertising and to minimize associated downsides while still enjoying the benefits of services of SC companies.

People often face serious challenges in their lives that are difficult or expensive to solve. Exposure to targeted advertising is not one of them. It is not particularly problematic to begin with, and there are inexpensive and simple, if imperfect, solutions available.<sup>33</sup>

<sup>29</sup> Raz, 1988, p. 156.

<sup>30</sup> As of April 2024. This also applies to Google’s web browser, Chrome, which no longer relies on third-party cookies. Note though that, even after an opt-out, Twitter/X will still show ads ‘based on your X activity’.

<sup>31</sup> Meaker, 2023a.

<sup>32</sup> Balebako et al., 2012; Gervais, Filios, Lenders, & Capkun, 2017; Merzdovnik et al., 2017.

<sup>33</sup> On irrational hostility towards advertising, see also McCloskey, 2019, pp. 120–121.

## 4 Surveillance Capitalism and Politics

While manipulative targeted advertising is often the primary complaint about surveillance capitalism, concerns about its impact on politics come in a close second. Allegations abound that surveillance capitalism negatively influences political culture, with Zuboff even claiming that we are in the midst of a 'death match' between democracy and surveillance capitalism.<sup>34</sup> Concerns about the political impact of surveillance capitalism merit serious attention. However, upon closer examination, the situation appears more nuanced and less dire.

The impact of surveillance capitalism on politics is a complex topic, and the already vast body of empirical research on it is rapidly growing. While I cannot cover every facet of its political impact, I will provide some evidence suggesting that some prominent worries might be exaggerated.

One such worry relates to the role of social media in spreading misinformation. A recent review of the academic discourse surrounding this concern portrays it as a moral panic. The authors summarize their findings as follows:

Unreliable news, including false, deceptive, low-quality, or hyper partisan news, represents a minute portion of people's information diet; most people do not share unreliable news; on average people deem fake news less plausible than true news; social media are not the only culprit; and the influence of fake news on large sociopolitical events is overblown.<sup>35</sup>

A literature review on echo chambers, filter bubbles, and polarization arrives at a similarly deflationary conclusion. The research reviewed suggests that "echo chambers are much less widespread than is commonly assumed, finds no support for the filter bubble hypothesis and offers a very mixed picture on polarisation and the role of news and media use in contributing to polarisation."<sup>36</sup> In fact, the authors note that there is some evidence suggesting that, contrary to what the filter bubble scare suggests, relying on search engines and social media for news consumption *increases* the diversity of people's news diet. Yet another review study confirms "that, rather counterintuitively, there is convincing empirical evidence demonstrating that social networking sites increase the range of political views to which individuals are exposed."<sup>37</sup> In the same vein, the author of a book-length treatment of this issue characterizes social media platforms as "important engines of context collapse, rather than enablers of ideological segregation", and concludes that, "[m]ainly, the debate about these concepts and their apparent impacts on society and democracy constitutes a moral panic."<sup>38</sup> The evidence regarding political

<sup>34</sup> E.g. Benn & Lazar, 2022; Coeckelbergh, 2024; Sunstein, 2018; Susser et al., 2019a, 2019b; Vaidhy-anathan, 2018; Véliz, 2020; Zuboff, 2022.

<sup>35</sup> Altay, Berriche, & Acerbi, 2023, p. 1 (references within the quoted paragraph were omitted).

<sup>36</sup> Ross Arguedas, Robertson, Fletcher, & Nielsen, 2022, p. 5.

<sup>37</sup> Barberá, 2020, p. 44.

<sup>38</sup> Bruns, 2019, pp. 99, 95–96. Similarly, an earlier review study concluded that "at present there is little empirical evidence that warrants any worries about filter bubbles" (Zuiderveen Borgesius et al., 2016, p. 1).

polarization is mixed. Some research supports the wide-spread belief that social media is exacerbating political polarization, possibly as a result of exposing users to opposing political views.<sup>39</sup> But a good deal of the literature challenges conventional wisdom. For instance, polarization has been found to be least pronounced among younger people, the demographic most likely to use social media.<sup>40</sup> There are even results suggesting that, precisely as a result of exposing users to a diversity of political messages, social media might be inducing political moderation rather than polarization.<sup>41</sup> One review study asserts that the “prevailing consensus in political science is that elite behavior, rather than communication, is driving political polarization.”<sup>42</sup> Another review concludes cautiously that the effect of social media use on polarization “remains unclear”, specifying that “in some cases social media exposure may exacerbate polarization while in other contexts or on certain platforms the effects are unobservable or even lead to depolarization.”<sup>43</sup>

The above does not amount to a comprehensive review of the sizeable body of literature on social media’s impact on filter bubbles, echo chambers, and polarization. And some of the results are inconclusive or contradictory. Still, the above discussion should suffice to make us pause and question one-sided alarmist narratives.

A related concern is political manipulation, where both the SC companies themselves as well as third parties using SC services or data could act as potential agents of manipulation. SC companies can wield considerable political influence since their algorithms can affect billions of users. Search engine companies can prioritize certain politically opportune results, social media companies can promote or suppress specific content, and so on. Given that most big tech companies lean to the left in terms of the composition of the staff of these companies, it is natural to suspect that SC companies might use their power to engage in left-leaning influencing and manipulation.<sup>44</sup> There is some evidence to suggest that this might be the case. Some high-profile cases of questionable left-leaning content curation include Twitter’s shadow-banning of Stanford Professor Jay Bhattacharya, a critic of the Covid lockdown measures, and its ban on gender-critical feminists, like philosopher Holly Lawford-Smith.<sup>45</sup> There are also studies suggesting a left-leaning bias of search engines.<sup>46</sup> However, a closer look reveals a less dramatic picture. For instance, the left-leaning bias reported by one of these studies consists in YouTube’s algorithms (which were found to steer users away from political extremes) to be more effective in steering users away from far-right content compared to far-left content.<sup>47</sup> Another

<sup>39</sup> Bail et al., 2018; see also Settle 2018.

<sup>40</sup> Boxell et al., 2017.

<sup>41</sup> Barberá, 2015; Beam et al., 2018.

<sup>42</sup> Tucker et al., 2018, p. 40; see also Arceneaux & Johnson, 2015.

<sup>43</sup> Kubin & von Sikorski, 2021, p. 194.

<sup>44</sup> Molla, 2018.

<sup>45</sup> Lawford-Smith, 2022; Stein, 2023. For an empirical documentation of shadow-banning, see Le Merrier, Morgan, & Trédan, 2021.

<sup>46</sup> Diakopoulous et al., 2018; Gezici et al., 2021; Ibrahim, AlDahoul, Lee, Rahwan, & Zaki, 2023; Kulshrestha et al., 2019; Lutz et al., 2021; Robertson et al., 2018.

<sup>47</sup> Ibrahim, AlDahoul, Lee, Rahwan, & Zaki, 2023.

study reporting a left-leaning bias in YouTube's initial search results found this bias to be 'slight' and that YouTube actively counteracts bias with its subsequent video recommendation.<sup>48</sup> A study that found a small left-leaning bias in Google's search engine, which is slightly more likely to produce left-leaning content, also revealed that Google's ranking algorithm tends to place left-leaning content further down the list of search results.<sup>49</sup> A study on Twitter/X and Google found some evidence of left-leaning bias, noting, however, that it "did not find evidence of any systemic bias, i.e., the platforms consistently ranking the items from one political leaning higher than the other, or consistently making the search results more polarizing by adding a Democratic-leaning bias to Democratic party related queries and Republican-leaning bias to Republican party related queries."<sup>50</sup> And a study that found Google and Bing search results to have a left-leaning bias also found these search engines to be unbiased for searches on specific controversial topics and notes that the bias that was found might not be attributable to biased algorithms.<sup>51</sup> Further evidence challenges the idea of a pervasive left-leaning bias among SC companies. A study that looked at comment moderation on YouTube found "no significant difference in moderation likelihood across the political spectrum."<sup>52</sup> The notion that online platforms intentionally stifle right-leaning voices is challenged by a forthcoming study on the news recommendations algorithms of Google, Facebook, YouTube and Twitter/X, which notes that right-leaning news sources "have received something of a bump in prominence."<sup>53</sup> An internal study by Twitter/X found that its personalization algorithms amplify right-leaning, rather than left-leaning, content.<sup>54</sup> Another yet-to-be peer-reviewed study indicates that any perceived political asymmetry in Twitter/X's enforcement of its anti-misinformation policy might simply reflect the differing tendencies among users to share misinformation based on their political leanings.<sup>55</sup> An official inquiry by the US Federal Election Commission, in response to concerns raised by the Republican National Committee, discovered no evidence that Google's spam filter had a bias against Republican fundraising emails.<sup>56</sup> Overall, while more research is needed, the available evidence paints a mixed and rather unremarkable picture. Some biases may exist, and we do well to monitor the activities of SC companies closely. But the evidence does not strongly support the idea that SC companies are systematically manipulating their user base politically. In fact, the practices of these companies appear rather even-handed when considered *in comparison*. For instance, they appear particularly even-handed when compared to other influential societal actors whose political biases are glaringly obvious, some of

<sup>48</sup> Lutz et al., 2021.

<sup>49</sup> Robertson et al., 2018.

<sup>50</sup> Kulshrestha et al., 2019, p. 222.

<sup>51</sup> Gezici et al., 2021.

<sup>52</sup> Jiang, Robertson, & Wilson, 2020.

<sup>53</sup> Nechushtai, Zamith, & Lewis, forthcoming, p. 20.

<sup>54</sup> Huszár et al., 2022. Similarly, A non-peer reviewed study by a SEO company on Google's search results suggests, if anything, a right-leaning bias (O'Toole, 2021).

<sup>55</sup> Mosleh, Yang, Zaman, Pennycook, & Rand, MS.

<sup>56</sup> Fung, 2023.

which even have a professional obligation to be impartial (think e.g. of media companies or supreme court justices). Presumably, SC companies' desire to maximize profit may be compatible with some bias, but it is incompatible with a pronounced political slant that would alienate a large proportion of the user base.<sup>57</sup> Considering the relatively low current level of political bias, regulatory efforts, which may invite partisan political influence, will probably increase rather than decrease bias and politicization.

The services or data from SC companies may also be tapped by third parties for potential political manipulation. Yet, the two most prominent scares about such interference have proven to be more bark than bite. The first case is the Russian social media campaign aimed at influencing the 2016 US election. A recent study found "no evidence of a meaningful relationship between exposure to the Russian foreign influence campaign and changes in attitudes, polarization, or voting behavior."<sup>58</sup> The other case is the Cambridge Analytica scandal. The evidence suggests that Cambridge Analytica grossly exaggerated its capability to sway voters, essentially duping naive politicians. Evidence of the efficiency of psychographic voter targeting is flimsy, as a *Nature* piece explains, making it unlikely that Cambridge Analytica's services had any significant impact on election outcomes.<sup>59</sup>

Not only have many of the problems been overstated. The services provided by SC companies might also impact politics in ways that most democratic theorists would welcome, e.g. by allowing people to express themselves politically and to organize political action.<sup>60</sup> Social media might be particularly valuable for emancipatory and anti-autocratic movements. Prominent examples that come to mind include the Arab Spring, in which social media seem to have played an important role,<sup>61</sup> and the Me-Too-movement. It is not entirely implausible to interpret the routine banning or limiting of access to SC services by autocratic regimes as indicative of their liberating potential.<sup>62</sup>

Against this backdrop, concerns that rampant political online manipulation threatens to erode collective autonomy by undermining individual autonomy appear exaggerated.<sup>63</sup> Both popular and scholarly discourse appear to be overestimating the extent and effectiveness of political online manipulation. Moreover, it is plausible that the services provided by SC companies can also have a positive effect on collective and individual autonomy. While its precise net effect on political autonomy is difficult to determine, it is not necessarily negative. All this is not to deny that

<sup>57</sup> See Caplan, 2022. For another more relaxed take on this issue, see Cowen, 2019, pp. 115–116.

<sup>58</sup> Eady et al., 2023, p. 1.

<sup>59</sup> Gibney, 2018; Karpf, 2019; Waterson, 2020. Contrary to a prevalent belief (e.g. Coeckelbergh, 2024, p. 38), Cambridge Analytica was not involved in the Brexit referendum (Waterson, 2020).

<sup>60</sup> See e.g. Jost et al., 2018.

<sup>61</sup> Steinert-Threlkeld, Mocanu, Vespignani, & Fowler, 2015.

<sup>62</sup> Note, though, that one study on the political effects of access to Facebook did not find any positive impacts in terms of regime changes in autocratic countries, improvements in indices of democracy, or measures of governance. It did find that access to Facebook leads to a decrease in violent internal conflict. (Fergusson & Molina, 2019).

<sup>63</sup> For a statement of this concern, see Susser et al., 2019a, 2019b.

there are political challenges associated with social media and other aspects of surveillance capitalism. Overall, the evidence bearing on this question is complex and often ambiguous or contradictory. However, the prevailing doomerist take on how surveillance capitalism impacts politics seems way off the mark. For one thing, it seems that the impact of social media on politics has been massively overstated. This assumption is further bolstered by a recent set of high-profile studies from the comprehensive Facebook and Instagram Election Study (FIES), conducted in partnership with Meta. These studies, where researchers tweaked the content that users were exposed to, suggest that social media algorithms simply have little impact on people's political attitudes and behaviour. As one commentator summarizes the results: "Participants didn't differ from other users in how polarized their views were, for example, or in their knowledge about the elections, their trust in media and political institutions, or their belief in the legitimacy of the election. They also were no more or less likely to vote in the 2020 election."<sup>64</sup> For another thing, to the extent that social media does have an impact on politics, its effects are not uniformly negative. Therefore, the notion that social media has a strong negative net effect on politics is difficult to sustain, let alone that its impact is obviously disastrous, as frequently suggested. Critics of surveillance capitalism who want to push this line of critique are facing a heavy empirical burden.

The above observations also allow us to respond to a more subtle version of the concern about the political impact of surveillance capitalism, which requires a more piecemeal discussion. This concern argues that surveillance capitalism is problematic because SC companies exert 'domination'. Within the neo-republican framework, political freedom is understood as the absence of domination, where domination refers to the uncontrolled exercise of power.<sup>65</sup> According to one statement of this neo-republican critique of surveillance capitalism, due to Williams and Raekstad, people suffer domination at the hands of SC companies because they are structurally forced to submit to SC companies' manipulative practices, which constitute a type of uncontrolled power.<sup>66</sup> This critique seems to unduly magnify the problem. First, nobody is 'forced' to use SC services. Choosing not to use them comes with trade-offs. But the situation is hardly comparable to the oft-cited scenario of a worker forced to sell their labor or face abject poverty. Second, as noted above, the effectiveness of online manipulation is generally being overestimated. Third, there exist various options for users to further reduce their vulnerability to manipulation, such as disabling cookies, blocking targeting ads, or browsing in incognito mode. Williams and Raekstad object that these measures are not 100% effective, which is true. But they still lead to a *substantial* reduction in one's exposure to the type of manipulation that ground concerns about domination. Fourth, the power exercised

<sup>64</sup> Kupferschmidt, 2023, p. 368; see Guess et al., 2023a, 2023b; Nyhan et al., 2023. Note, though, that the fourth study from this series found considerable ideological segregation on Facebook and that algorithmic curation plays at least some role in this (González-Bailón et al., 2023).

<sup>65</sup> Pettit, 2014.

<sup>66</sup> Williams & Raekstad, 2022, similarly Aytac, 2024; Hoeksema, 2023; Oldenbourg, 2024; Taylor, 2021.

by these companies is not ‘uncontrolled’. The fact that users can readily abandon a specific service—either migrating to a competitor or opting out entirely—introduces a direct accountability mechanism. SC companies’ strong financial interest in retaining their user base gives users a tangible degree of control over them. Finally, it is again worth considering potential *positive* effects of surveillance capitalism on people’s freedom understood as non-domination. Even if SC companies did exercise *corporate* domination over their users, neo-republicans might find that the services they provide counteract *political* domination. As noted above, they offer services that can empower people suffering political oppression. All things considered, it is questionable whether the domination asserted by SC companies is substantial enough to be worth losing sleep about. Furthermore, a complete neo-republican assessment of SC should evaluate its *net* impact on freedom as non-domination, which could well be positive.

## 5 Surveillance Capitalism and Mental Health

Another worry that has emerged in recent years pertains to mental health. A substantial body of evidence suggests that we are in the midst of a mental health crisis, marked by increased rates of anxiety disorders, depression, self-harming behavior, and suicide. The crisis primarily affects adolescents, with young women tending to be more severely affected than young men.<sup>67</sup>

The adolescent mental health crisis is somewhat of a scientific mystery, with psychologists puzzled over what developments might causally account for it. One potential culprit is the use of smartphones and social media. Supporting this hypothesis is the temporal connection between the emergence of the mental health crisis and the adoption of smartphones among young people, both starting in lockstep in the early 2010s. Additionally, there are various reasons why the mental health impact of social media may be assumed to be worse for young women. For instance, young women are more vulnerable to harm from visual social comparison, they are more likely to engage in and experience relational (as opposed to physical) aggression, and they spend more time on social media.<sup>68</sup>

The hypothesis that the use of smartphones, especially social media, is accountable for the mental health crisis is prominently defended by Jonathan Haidt. As the subtitle of his recent book *The Anxious Generation* reveals, he believes that ‘the great rewiring of childhood is causing an epidemic of mental illness’. Interpreting the large body of empirical research, Haidt suggests that the algorithms of social media companies are effectively drawing socially insecure young users, with their immature frontal cortices, into a quagmire of mental toxicity.<sup>69</sup> If Haidt’s account is correct, it would cast a very bad light indeed on surveillance capitalism, specifically

<sup>67</sup> See e.g. Burstein et al., 2019; Keyes et al., 2019; Twenge, et al., 2019; for reviews, refer to Haidt, 2024, ch. 1; Haidt et al., ongoing; Twenge, 2023, p. 392–400.

<sup>68</sup> Haidt, 2024, ch. 6.

<sup>69</sup> Haidt, 2024; similarly, Twenge, 2023, pp. 392–416.

its social media branch. If companies like Facebook or Instagram are single-handedly responsible for a serious mental health epidemic among youths, their business practices are hard to defend.

However, it is doubtful that Haidt's narrative is borne out by the available empirical evidence. While some research supports his pessimistic view of social media's impact on mental health,<sup>70</sup> it is contradicted by several meta-analyses, review studies, and umbrella studies (reviews of review studies). A meta-analysis, aptly titled '*Like This Meta-Analysis*,' concludes that "there does not appear to be robust evidence to suggest that screen time is associated with, let alone a cause of, mental health problems," a finding that also held specifically for social media use.<sup>71</sup> Another meta-analysis of studies on social media and mental health found the mean effect sizes to be "no different from zero", noting however a considerable heterogeneity in effect sizes across studies.<sup>72</sup> A meta-analysis and review study on social media use and self-injurious thoughts and behavior concludes that "no significant associations were identified between frequency of social media use and suicidal ideation, plans, nor [nonsuicidal self-injury]".<sup>73</sup> A review study on adolescent mental health and digital technology notes that "the most recent and rigorous large-scale preregistered studies report small associations between the amount of daily digital technology usage and adolescents' well-being that do not offer a way of distinguishing cause from effect and, as estimated, are unlikely to be of clinical or practical significance."<sup>74</sup> An umbrella study on the topic, offering a synthetic review of several meta-analyses and review studies, points out that "most reviews interpreted the associations between social media use and mental health as 'weak' or 'inconsistent'."<sup>75</sup> Another umbrella study similarly found that "the association between digital technology use, or social media use in particular, and psychological well-being is – on average – negative but very small."<sup>76</sup> As Candice Odgers, a leading researcher in the field, puts it in her review of Haidt's book, the "suggestion that digital technologies are rewiring our children's brains and causing an epidemic of mental illness is not supported by science."<sup>77</sup>

The notion that it is bad for people's mental health to spend many hours per week doomscrolling on social media is intuitively compelling. But the empirical evidence on this issue is again ambivalent, to say the least. It does not provide clear support for the alarmist narrative pushed by Haidt and other critics of social media companies. That being said, we should monitor this issue closely. Concerns about the negative impacts of social media use on mental health should be taken seriously. Given

<sup>70</sup> E.g. Braghieri et al., 2022; Brailovskaia et al., 2020; Twenge, 2020. Refer to Haidt's book for more.

<sup>71</sup> Ferguson et al., 2020, p. 212.

<sup>72</sup> Ferguson, forthcoming, p. 5.

<sup>73</sup> Nesi et al., 2021, p. 11. The authors note, however, that there are only few studies investigating these associations (ibid.).

<sup>74</sup> Odger & Jensen, 2020, p. 336.

<sup>75</sup> Valkenburg et al., 2022, p. 58.

<sup>76</sup> Orben, 2020, p. 407; for even more umbrella studies pointing in a similar direction, see Appel et al., 2020; Meier & Reinecke, 2020.

<sup>77</sup> Odgers 2024, p. 29.

the difficulty of studying the phenomenon,<sup>78</sup> the vastness of the available empirical literature,<sup>79</sup> the questionable quality of some of the existing research,<sup>80</sup> as well as some expert disagreement about its significance, it would be premature to dismiss these concerns as entirely unfounded. It is to be hoped that future research will provide a more conclusive understanding of the mental health implications of social media use.<sup>81</sup>

## 6 Surveillance Capitalism and Government Surveillance

Barring some exceptions, surveillance capitalism does not typically involve surveillance, at least not in the most natural sense of the term. This does not mean that the data collected by these companies for their own (mostly non-surveillance) purposes cannot be used for surveillance by third parties. One criticism raised against surveillance capitalism is that it facilitates objectionable instances of government surveillance. Recent decades have witnessed a vast expansion of government surveillance, as notoriously revealed by Edward Snowden in the mid-2010s. Despite the public outcry this provoked, the appetite for surveillance by governments has barely diminished since. The expansion of government surveillance has sparked significant concern, with many commentators considering the extent and nature of contemporary government surveillance deeply problematic.<sup>82</sup> Companies involved in surveillance capitalism have drawn criticism for their enabling role in these disconcerting surveillance practices. Critics of SC companies have painted them as compliant collaborators, willingly aiding governments in their excessive and unaccountable surveillance endeavors.<sup>83</sup>

This criticism of SC companies is based on the assumption that government surveillance is inherently bad. One possible response to this criticism could therefore be to defend government surveillance. Such a defense would portray SC companies' participation in government surveillance as desirable. In my view, there is a kernel of truth to this response. Even the most outspoken critic of government surveillance will admit that *some* forms of government surveillance are necessary and desirable. A state incapable of monitoring the adherence to its laws would cease to be functional. However, it is also undeniable that many instances of government surveillance *are* worrisome, whether due to their vast scale, lack of accountability, or both.

<sup>78</sup> See Dahl et al., unpublished.

<sup>79</sup> See Haidt et al., ongoing, to get an idea of the vastness of the literature.

<sup>80</sup> See Orben, 2020, who diagnoses a “lack of high-quality research in the area” (p. 407); see also Ferguson, forthcoming.

<sup>81</sup> Suggestions for future research are made, e.g., in Ferguson, forthcoming, Orben, 2020; Valkenburg, 2022; Valkenburg et al., 2022.

<sup>82</sup> For some critical takes on government surveillance, see Hoyer & Monaghan, 2018; Königs, 2022; Macnish, 2018b; Roberts, 2015; Stahl, 2016.

<sup>83</sup> E.g. Véliz, 2020, pp. 40–50; Zuboff, 2019, pp. 112–121, p. 385; see also Vaidhyanathan, 2018, pp. 61–62.

I therefore consider the concern that SC companies enable objectionable government surveillance to be legitimate and important.

It is not possible to dispel this concern entirely. The fact that SC companies accumulate vast amounts of data carries the risk of these data being misused by governments, a danger that trivially did not exist before the rise of data collecting internet giants. However, the role of SC companies in government surveillance is much more ambivalent than widely presumed. Critics can point to instances where technology companies have willingly collaborated with surveilling governments in ways that raise ethical red flags. Specifically, it seems that telecommunications companies Verizon and AT&T have cooperated extensively and voluntarily with the NSA.<sup>84</sup> However, contrary to a widespread myth, this does not appear to apply to the major SC companies (Google, Facebook, Yahoo, etc.). The widely held belief that the NSA could directly access the servers of large SC companies as part of the PRISM program and that these companies facilitated this willingly, does not seem supported by the available evidence.<sup>85</sup> Moreover, the relationship between big technology companies and government agencies is becoming increasingly adversarial. As Rozenshtein observes: "Never in the history of electronic surveillance have technology companies so aggressively stood up to the government. [...] [T]he age in which technology companies would salute smartly to government surveillance orders is over."<sup>86</sup> Along the same lines, another commentator, describing the "recent trend of increased hostility" between government and Big Tech, points out: "In contrast to the voluntary cooperation seen in the years immediately following 9/11, today's surveillance intermediaries generally do not hand over data unless the government utilizes formal legal processes to compel its production."<sup>87</sup> Examples of tech companies pushing back against government surveillance include open calls for limiting government surveillance,<sup>88</sup> the implementation of end-to-end encryption,<sup>89</sup> Apple's repeated refusal to assist law enforcement agencies in unlocking terrorists' smartphones,<sup>90</sup> SC companies' legal challenges to gag orders that prevent them from disclosing government requests for user data,<sup>91</sup> their refusal to sell facial recognition technology to the police in the absence of adequate regulation of this technology,<sup>92</sup> and their resistance to

<sup>84</sup> Gustin, 2013; Harvard Law Review Staff, 2018, p. 1725.

<sup>85</sup> One commentator describes the situation as follows: "The botched reporting by the Guardian and the Post means that millions of readers directed their anger at a handful of big companies that were unfairly accused of selling out their customers to the national security apparatus. The reality is that if NSA surveillance is indeed overstepping its bounds, those companies are victims, not willing participants." (Bott, 2013) See also Braun, Flaherty, Gillum, & Matt Apuzzo, 2013; Harvard Law Review Staff, 2018, pp. 1728–1729; Eichenwald, 2013; Rozenshtein, 2018, p. 116 n73.

<sup>86</sup> Rozenshtein, 2018, pp. 121–122.

<sup>87</sup> Izant, 2017.

<sup>88</sup> Wyatt & Miller, 2013.

<sup>89</sup> Gupta, 2020.

<sup>90</sup> Holpuch, 2016; Morrison, 2020.

<sup>91</sup> Solon, 2017; "Victory: U.S. won't try to gag Facebook from telling users about warrants for their data," 2017.

<sup>92</sup> Heilweil, 2020.

government data requests that lack adequate legal authority.<sup>93</sup> One part of the explanation for their resistance, Rozenshtein suggests, is the tangible economic incentives provided by their users' desire for privacy. As one commentator observes, "[t]he Snowden leaks changed the behavior of communications companies. Firms began to compete, in part as a marketing move, to be seen as protecting the security of users' private messages."<sup>94</sup> Another part of the explanation might be ideological motives rooted in Big Tech's libertarian-leaning culture.<sup>95</sup>

Again, it is true that, because of the rise of surveillance capitalism, governments' surveillance capacities have expanded, as they can now compel SC companies to hand over data. But the relationship between SC companies and surveilling governments is more adversarial than widely believed. More often than not, SC companies push back against government surveillance efforts. When they do share data, they often do so grudgingly and under coercion. That being said, it is important to acknowledge the ambivalence of the issue. SC companies are no angels, and it would be wrong to portray their behavior as invariably and uniformly adversarial.<sup>96</sup> For instance, it recently emerged that Twitter/X is still collaborating with Dataminr, a company that offers surveillance services to US law enforcement.<sup>97</sup> Moreover, the intelligence world is inherently murky, making reliable assessments of the involvement of SC companies difficult. Lastly, on an ethical level, it is not always clear when an SC company's refusal to collaborate with law enforcement is praiseworthy and when it is wrong.<sup>98</sup>

## 7 Surveillance Capitalism, the Rule of Law, and Social Trust

Another concern, again prominently voiced by Zuboff, is that certain manifestations of surveillance capitalism undermine the rule of law and social trust. According to Zuboff, this occurs when collected data is used for the purpose of monitoring contract compliance. For instance, car insurance companies can use surveillance data to check whether their customers are driving safely, as stipulated in the insurance contract. Similarly, surveillance data can be used to monitor whether a person contracted for a job in a remote location is fulfilling their contractual obligations. Such instances of surveillance capitalism, originally proposed by Google's chief economist Hal Varian as *positive* examples of the utility of Big Data, lead to an erosion of the rule of law and social trust, according to Zuboff.<sup>99</sup> This dimension of surveillance capitalism does not constitute the core business of major SC players and lies somewhat at the periphery of surveillance capitalism proper. Nevertheless, I want

<sup>93</sup> Ireland, 2021.

<sup>94</sup> Savage, 2017, p. 570.

<sup>95</sup> Rozenshtein, 2018, pp. 115–119.

<sup>96</sup> See Harvard Law Review Staff, 2018.

<sup>97</sup> Biddle, 2024.

<sup>98</sup> For a discussion, see Etzioni, 2018.

<sup>99</sup> Varian, 2014; Zuboff, 2015, pp. 81–83.

to briefly address this concern here. One reason it deserves our attention is that this indeed constitutes a genuine case of surveillance in the above suggested sense of the term. Collected data are used to ensure compliance with certain expectations (in this case: contracts).<sup>100</sup>

First, then, Zuboff argues that this form of surveillance leads to the undermining of the rule of law and even makes the institution of contract itself obsolete: "Surveillance capitalism establishes a new form of power in which contract and the rule of law are supplanted by the rewards and punishments of a new kind of invisible hand."<sup>101</sup> It is not easy to make sense of this claim. It is unclear why the data-based verification of contract compliance should spell the end of the institution of contract, or even represent an 'un-contract', as Zuboff terms it.<sup>102</sup> Surely, a contract is no less a contract if the parties involved can avail themselves of reliable means of verifying compliance, such as data-based monitoring. Similarly, it is not evident why the data-based verification of contract compliance should threaten the rule of law. Francis Fukuyama mentions three different definitions of the rule of law: 1) A system in which the rulers are bound by a higher law, e.g., by a constitution. 2) A system that guarantees property rights and the enforcement of contracts. 3) A system in which people's physical safety is guaranteed, that is, where they need not fear being killed or robbed.<sup>103</sup> The rule of law, according to the first and third definitions, is not affected by the data-based monitoring of contract compliance. If we use the second definition, data-based monitoring of contract compliance *supports* the rule of law precisely because it facilitates contract enforcement. On a more charitable interpretation, Zuboff may mean that the rule of law is at risk because surveillance capitalists, or companies using their data, can enforce the contracts themselves, effectively acting as judge in their own cause. She mentions the possibility that a car rental company might instruct the vehicle monitoring system to prevent a delinquent customer from starting the car, or that a car insurance company might shut off a car if the customer is driving too fast. In Zuboff's view, the problem seems to be that we are here dealing with a "privately administered compliance regime".<sup>104</sup> However, this criticism overlooks the fact that the right to such data-based interventions can itself be contractually established. There is nothing anti-rule of law or 'un-contract'-like about specifying in a contract that the service provided will be automatically discontinued if, say, the customer fails to comply with certain safety standards. The company would not thereby place itself above the law, and customers retain the right to pursue legal recourse if they feel that a breach of contract has occurred. Moreover, the possibility of making such arrangements can be socially beneficial, e.g. by lowering insurance premiums and encouraging responsible driving.

<sup>100</sup> One issue not discussed here concerns the ethics of data-driven *pricing* (on this, see e.g. Seele, Dierksmeier, Hofstetter, & Schultz, 2021; Steinberg, 2022).

<sup>101</sup> Zuboff, 2015, pp. 82.

<sup>102</sup> Zuboff, 2015, pp. 81; 2019, pp. 217–220.

<sup>103</sup> Fukuyama, 2011, pp. 247–251. He prefers the first.

<sup>104</sup> Zuboff, 2015, pp. 83.

Second, Zuboff fears that data-based monitoring of contract compliance leads to an erosion of social trust, as it “eliminates the need for – and therefore the possibility to develop – trust.”<sup>105</sup> The assumption seems to be that as opportunities to verify compliance with contractual obligations increase, social trust decreases. This, however, is a speculative empirical hypothesis, and Zuboff fails to substantiate it with any evidence. If anything, there is evidence suggesting the opposite might be true. In their study on trust and economic growth, Paul Zak and Stephen Knack found that trust *increases* with the existence of formal institutions that allow detecting and punishing cheaters.<sup>106</sup> Also, as a side note, with the annual costs of insurance fraud in the US exceeding 40 billion dollars,<sup>107</sup> the idea that insurance companies should simply *trust* their customers seems naive.

To Zuboff, a world in which Big Data helps ensure compliance with contracts resembles.

an arid wasteland – not a community of equals bound through laws in the inevitable and ultimately fruitful human struggle with uncertainty. In this futurescape, the human community has already failed. It is a place adapted to the normalization of chaos and terror where the last vestiges of trust have long since withered and died.<sup>108</sup>

The hyperbolic rhetoric contrasts sharply with the low plausibility of these claims and the scant evidence offered in their support.

## 8 Surveillance Capitalism and Privacy

One key theme in debates surrounding surveillance capitalism is privacy. Many critiques of surveillance capitalism are formulated within a privacy framework. The massive erosion of privacy that surveillance capitalism is deemed to have caused is often mentioned as one of its ‘dark sides’.<sup>109</sup> Again, while the privacy concern contains more than just a grain of truth, a closer look reveals a more ambivalent and less dramatic picture.

To begin with, it is important to note that the extent to which a given practice should be seen as privacy-reducing depends on what is meant by privacy. In my view, the most plausible account of privacy is the access account. According to the access account, privacy is not diminished unless human access to data takes place.

<sup>105</sup> Zuboff, 2015, pp. 81.

<sup>106</sup> Zak & Knack, 2001. Relevant in this context might also be the literature demonstrating a positive link between market integration/capitalism and trust/prosocial behaviour (for an overview, see Brennan, 2014, pp. 65–69). Given that a) market integration seems to promote trust and b) surveillance capitalism might enable previously impossible market transactions, one would, if anything, expect a *positive* effect on trust.

<sup>107</sup> Insurance Fraud.

<sup>108</sup> Zuboff, 2015, p. 81.

<sup>109</sup> A go-to reference here is Véliz, 2020, who frames her entire critique of the industry as a privacy issue.

Macnish offers a powerful thought experiment in support of the access account. A person forgets her diary in a coffee shop. When she returns to the coffee shop to pick up the diary, she learns that it was in the possession of a stranger. Fortunately, the stranger had the decency not to open the diary. Intuitively, although the diary owner's 'data' were in somebody else's possession, her privacy seems to have remained intact. A loss of privacy would have occurred only if the stranger had opened and read the diary. This suggests that a person's privacy is only reduced if actual access to information takes place.<sup>110</sup> If the access account is correct, the assumption that mass surveillance, whether by government agencies or big tech companies, has caused a massive erosion of privacy is false. As Macnish points out, government surveillance involves the collecting of huge amounts data but little actual access.<sup>111</sup> The same is true of 'surveillance' by tech companies.<sup>112</sup> It is very unlikely that someone is personally reading your emails or WhatsApp messages, scrutinizing your Google search prompts, or judging your YouTube habits. The collection and processing of these data are performed by computers, not humans. The placement of targeted advertisements, for instance, is entirely automated. It does not involve an employee of an SC company personally sifting through your browser history and deciding which product you might be interested in. Therefore, if access is required for a loss of privacy to occur, SC companies' collecting and using massive amounts of user data does not translate to a massive reduction in people's privacy.<sup>113</sup> To be sure, unwanted human access to collected data does occasionally occur, for instance, when user data are leaked or hacked. It would be incorrect to claim that surveillance capitalism never results in reductions in privacy involving unwanted access to personal information. But for any individual using SC services, the risk of this happening to them is relatively low. You can use SC services without having to worry too much about unwanted human access to your personal information. Presumably, this is a reason why so many people happily use these services, even though they are averse to unwanted access to their personal data. They know that the likelihood of someone actually accessing their personal data, while not zero, is small.

What is more, we must also take into account surveillance capitalism's positive effects on people's privacy (understood along the lines of the access account of privacy). With surveillance capitalism routinely condemned for having dealt the death blow to privacy, the notion that it could have a positive impact on privacy seems outlandish. However, a strong argument can be made that the services provided by SC companies do in fact protect people's privacy in certain ways. SC services have made it much easier for individuals to learn about and discuss topics without needing to disclose their identity or engage with others in person. The benefits of this are particularly great when it comes to sensitive topics, such as issues related to sex and relationships, mental and physical health, or personal finances. Search engines

<sup>110</sup> Macnish, 2018b; see also Sorell, 2018.

<sup>111</sup> Macnish, 2018b; see also Sorell, 2018.

<sup>112</sup> Macnish, 2020.

<sup>113</sup> Note that certain versions of the control account of privacy, a rival to the access account, might have the same implications (Menges, 2020).

enable users to access a wealth of detailed and reliable information on virtually any topic of interest. Moreover, internet forums, which are often financed through targeted advertising and free to use, allow individuals to discuss sensitive and less-sensitive issues pseudonymously, by sharing their own experiences and learning from the experiences of others. Without these services, discussing and learning about sensitive topics would be associated with significant privacy costs.<sup>114</sup> The enormous popularity of such services is undoubtedly in no small part due to the protection they afford to users' privacy.

I do not claim to be able to definitively determine whether the net impact of surveillance capitalism on people's privacy is positive or negative. Balancing the privacy costs against the privacy benefits is difficult. The 'privacy calculus' may also vary from user to user as a function of their interests, values, and internet usage habits. Nonetheless, we can say that surveillance capitalism performs better in terms of privacy than its critics often suggest.<sup>115</sup>

Some critics of surveillance capitalism will find these points unconvincing. While 'privacy' frequently remains undefined in debates about surveillance capitalism, it is clear that many critics use the term in a looser sense. They take the mere collecting, and perhaps processing and using, of data to constitute reductions in privacy, even when no access takes place. It is the aggressive 'data grabbing' by SC companies that is taken to erode our privacy, whether data are accessed or not. What can be said in response to critics who rely on such a more permissive notion of privacy?

One response is that the presence or absence of access matters ethically. The fact that human access to the collected data is fairly limited is a good thing. There is something distinctly unpleasant about other people accessing personal information without our consent. Consider again the diary case. It would have been much worse if the finder of the diary had read it. Given the plausibility of the access account and the limited access taking place, the case can be made that surveillance capitalism has not resulted in the complete annihilation of privacy, contrary to frequent suggestions. But even if one rejects the access account, the fact that access is limited carries intrinsic ethical significance. Whether we take access to be relevant on a definitional level, on an ethical level the fact that access is rare is an important remedying factor. That is why people are happy to use these 'data grabbing' services. To them, (non-)access matters.<sup>116</sup>

Another response relates to the function of privacy understood in this looser, more encompassing sense. Critics bemoaning the loss of privacy brought about by surveillance capitalism tend to conceive of privacy, understood in this broader sense, as a bulwark against certain evils associated with surveillance capitalism. For instance, Williams and Raekstad stress that "one of the reasons why informational privacy is

<sup>114</sup> As Caplan notes, "[f]or practical purposes, we have more privacy than *ever before in human history*. You can now buy embarrassing products in secret. You can read or view virtually anything you like in secret. You can interact with over a billion people in secret." (2019). On the idea that technological progress in general has enhanced our 'social' privacy, see Garfinkel, 2020.

<sup>115</sup> As a reviewer points out, merely counting the 'positive' and 'negative' effects might be unsatisfactory. The changes in privacy do not only have a quantitative but also a qualitative dimension. The kind of privacy we have today is *different*.

<sup>116</sup> See also Königs (2022), pp. 8–9.

important to republicans is that it safeguards against certain forms of manipulation and thus domination.”<sup>117</sup> Similarly, Véliz observes that “[p]rivacy protects us from unwanted pressures and abuses of power. We need it to be autonomous individuals, and for democracies to function well we need citizens to be autonomous.”<sup>118</sup> Here, privacy seems to be used in a looser sense, where ‘data grabbing’ itself constitutes a loss of privacy. Privacy is valued as a protector against certain evils. To some extent, I agree with this perspective. But it means that the concern about privacy, thus understood, might not be best treated as an additional concern in its own right, over and above concerns about targeted advertising, political manipulation, mental health issues, etc. Rather, it is dependent on the seriousness of these other concerns. To the extent that these concerns are less serious or real than assumed, the loss of privacy, in this more permissive sense, is also less serious. This is what I cautiously suggest might be the case. Many concerns that loom large in critiques of surveillance capitalism, against which privacy may protect us, appear to be less dramatic than critics have us believe. Therefore, the erosion of privacy (if we want to call it that) caused by the mere collection and processing of data is also less concerning.

Again, I am not suggesting that SC companies acquiring vast amounts of data about their users does not warrant concern or scrutiny. This would be to lapse back into the black-and-white thinking that we should avoid. But overall, privacy is not in as dire a state as the prevailing narrative suggests. Technically, it is not even clear that a massive erosion of privacy has taken place, given that actual access seems like a reasonable condition for loss of privacy and that SC services also provide privacy benefits to their users. Moreover, concerns about erosions of privacy, understood in a looser sense, are mitigated by the fact that fears about the consequences of these erosions may be exaggerated.<sup>119</sup>

## 9 The Perks of Surveillance Capitalism

Surveillance capitalism has gotten a bad rep in both scholarly and popular debate. This negative narrative arises in large part because the negative aspects of surveillance capitalism have been exaggerated. I have tried to demonstrate in previous sections that some common concerns and objections are overblown. Another reason for the negativity is that the benefits are rarely acknowledged. Critics of surveillance capitalism arrive at a dystopian picture by focusing on its associated (real or imagined) problems while largely overlooking the benefits of SC services. Such an approach inevitably results in an incomplete and overly negative view. *Any* phenomenon will appear problematic if, in our analysis, we focus solely or primarily on its negative aspects. For an accurate picture of surveillance capitalism, we must consider not only its downsides but also potential positive aspects.

<sup>117</sup> 2022, p. 422.

<sup>118</sup> 2020, p. 90.

<sup>119</sup> It is worth noting that for some privacy concerns, users can again resort to quick and fairly effective fixes, which include those discussed above for reducing exposure to targeted advertising as well as the use of a VPN client.

The positive aspects are the benefits that SC services provide to users. As one of the rare enthusiasts about these companies puts it:

Facebook, Twitter, and other social media let us socialize with our friends, comfortably meet new people, and explore even the most obscure interests. The price: free. [...] Youtube gives us endless entertainment. The price: free. Google gives us the totality of human knowledge! The price: free.<sup>120</sup>

Even though the services are only *almost* free (users exchange their data), the observation is fundamentally correct. SC companies offer immense benefits to their users virtually for free. And the list could be spelled out even further. Social media does not only allow us to socialize with our friends and explore our interests but also provides opportunities for professional networking and career development. YouTube does not just provide free entertainment, but also free education, tutorials, product reviews, and much more.<sup>121</sup> Google does not merely offer us the totality of human knowledge (Google Search, Google Scholar) but also worldwide navigation (Google Maps) as well as tools for communication (Gmail) and collaboration (Google Docs), among various other services. Besides the products offered by these SC giants, there are countless smaller SC companies providing users with a diverse range of services. It is worth stressing that these go beyond just entertainment. Popular app categories in Google's and Apple's app stores include such categories as Education (some 10% of all apps), Business, Health & Fitness, Productivity, and Finance.<sup>122</sup>

The value of these services to consumers has been estimated by studies that sought to determine consumers' 'willingness to accept' (WTA) valuations. This metric represents the monetary compensation they would require for temporarily losing access to the specified good or service. One study estimated the median WTA for one year to be as high as \$17,530 for all search engines, \$8,414 for all email services, \$3,648 for all mapping services, and \$333 for all social media platforms.<sup>123</sup> A similar study from 2018 found that "the mean bid to deactivate Facebook for a year exceeded \$1,000." The authors conclude that "even the most conservative of these mean WTA estimates, if applied to Facebook's 214 million U.S. users, suggests an annual value of over \$240 billion to users".<sup>124</sup>

Such estimates are difficult and should be taken with a grain of salt. Still, it is arguable that SC services hold significant value for their users. The above figures indicate a substantial consumer surplus, contradicting Zuboff's claim that

<sup>120</sup> Caplan, 2019; similarly, Norberg 2023, ch. 5.

<sup>121</sup> Educational videos, tutorials and product reviews are among the most popular online videos, although the market is largely dominated by entertainment (Ceci, 2023; see also Cowen, 2019, p. 108).

<sup>122</sup> Ceci, 2022a, 2022b.

<sup>123</sup> Brynjolfsson, Collis, & Eggers, 2019.

<sup>124</sup> Corrigan, Alhabash, Rousu, & Cash, 2018, p. 7.

“surveillance capitalists create value, but the value is for them.”<sup>125</sup> Of course, not all SC services are equally valuable. I find it plausible that some people should spend (a lot) less time on social media. The monetary value they assign to access to social media might well exceed its actual value for personal flourishing. It is conceivable that one reason why they are willing to pay money to retain access to social media is because *others* are using social media and they do not want to be feel left out.<sup>126</sup> For this reason, social media may be less valuable than WTA studies suggest. The main point, however, which has both a methodological and a substantive component, remains. Methodologically, it is wrong to depict surveillance capitalism as a great evil based solely on an account of its (real or imagined) negative aspects. We must also take into account that SC companies benefit their users by offering them valuable services in return. The substantive point is that the value of these services is indeed considerable, even if their value is difficult to determine with precision, and even if some services are more beneficial than others.

## 10 Conclusion

If my analysis is roughly on track, the prevailing dystopian narrative regarding surveillance capitalism is misguided. The dangers associated with surveillance capitalism have been exaggerated, and its benefits have not been sufficiently recognized.

This does not mean that there are no valid concerns at all or that we should refrain from critically scrutinizing SC companies. My analysis, both of the potential problems as well as the benefits of surveillance capitalism, is also by no means exhaustive. I have focused on a selection of concerns and objections that figure prominently in academic and popular discourse. This selection is incomplete. Potential concerns I have not discussed include monopolistic tendencies in the SC sector,<sup>127</sup> the notion that surveillance capitalism is ‘colonialist’,<sup>128</sup> and problems that might only arise in the future, as SC companies continue to accumulate data and data-based power. These and other issues remain undiscussed, and I merely flag them here as topics for future discussion. Likewise, I do not take my analysis to be definitive. Given the complexity of some of the empirical questions, the conclusions drawn in this essay should be viewed as tentative and preliminary. Surveillance capitalism is a phenomenon in flux, with many parameters — technological developments, regulatory frameworks, corporate policies, user habits, and so forth — continuously

<sup>125</sup> Zuboff, 2022, p. 28. They also call into question the notion that users of SC companies are being exploited in a concerning way (as suggested by Benn & Lazar, 2022; Venkatesh, 2021).

<sup>126</sup> As an unpublished working paper suggests (Bursztyjn et al., 2023).

<sup>127</sup> Srnicek, 2017; but see also Cowen, 2019, pp. 103–107.

<sup>128</sup> Meijias & Couldry, 2024.

evolving.<sup>129</sup> The rapid advancement of AI technologies is one such technological development that could substantially alter the dynamics of surveillance capitalism. Finally, some of the developments discussed here might be associated with transformations on a qualitative level not captured by the convenient but simplistic framing in terms of ‘negatives’ and ‘positives’.

That being said, I believe that the above discussion provides good reason to be more relaxed about surveillance capitalism. I take this result to be intrinsically interesting and hope that it offers a useful lens for future discussion of this topic. Rectifying the negative narrative around surveillance capitalism is also important for practical reasons. Generally speaking, raising alarm about a technological development that, upon closer inspection, does not warrant such alarmism is likely not conducive to progress, whether social or technological. Being overly concerned about surveillance capitalism and related phenomena can lead to various adverse outcomes, aside from discouraging people from using and benefiting from SC services. For example, it has been noted that unwarranted ‘techno panics’ can produce harmful secondary effects. Although Cambridge Analytica and the Russian foreign influence campaign appear to have failed to directly sabotage democratic processes, their perceived effectiveness in the eyes of the public has likely led to diminished trust in the electoral system.<sup>130</sup> One may therefore question whether it benefits liberal democracies to stoke panic about social media and surveillance capitalism in the absence of sufficient evidence of an effect that might justify such concern. Unjustly blaming SC companies for all kinds of societal problems is ill-advised also because it obstructs addressing the real causes of these issues. Some of these problems – e.g., political dysfunction or the adolescent mental health crisis – may have causes that are unrelated to technology use, in which case we will fail to remedy them by scapegoating technology companies.<sup>131</sup>

Finally, misconceptions about surveillance capitalism are also troubling when considering regulatory actions. Many scholars and commentators call for comprehensive regulation of Big Tech. These calls for regulation are likely based, in part, on the widespread perception that surveillance capitalism poses a serious threat to our society. If this perception is incorrect, the extent of sensible and permissible regulation might be much less than commonly assumed. There is a powerful general presumption against government regulation, both on account of its moral costs (it is coercive) and its practical costs (it tends to lead to unintended consequences and inefficiencies, stifle innovation, bloat the bureaucracy, be costly to implement and enforce, invite rent seeking, etc.).<sup>132</sup> This means that regulation needs to be

<sup>129</sup> In fact, it has been suggested that recent EU rulings have marked the beginning of the decline of surveillance capitalism (Meaker, 2023b; see also Claburn, 2023; Goujard, 2023). Whether this is the case remains to be seen.

<sup>130</sup> Eady et al., 2023, p. 9; see also Altay & Acerbi, forthcoming; Altay et al., 2023. On techno panics, see Orben, 2020.

<sup>131</sup> Bruns, 2019, ch. 5.

<sup>132</sup> For related concerns, see Chomanski, 2021. For one example of how *prima facie* desirable regulation can have unintended negative repercussions, see Kircher and Foerderer’s study on how banning targeted advertising stifles innovation (2024).

well-justified. If the pessimistic narrative about surveillance capitalism is false, the stringent criteria needed to justify such regulations will often not be met. But it is not just about the *extent* of legitimate regulation, it is also about its *quality*. Even if there is legitimate ground for regulation, regulatory efforts that are based on misconceptions about surveillance capitalism are unlikely to improve the situation. As the authors of a review study on filter bubbles put it: “One lesson we should have learned from the past is that panic does not lead to sane policies.”<sup>133</sup> Zuiderveen Borgesius et al., 2016, p. 11.

**Acknowledgements** For helpful feedback and discussions, I would like to thank Tobias Blase, the members of the ‘Explainable Intelligent Systems’ research group, as well as audiences at the DKPhil in Münster, Frankfurt School of Finance and Management, Ruhr University Bochum, and RWTH Aachen University.

**Funding** Open Access funding enabled and organized by Projekt DEAL. The author declares that no funding was received during the preparation of this manuscript. The author has no relevant financial or non-financial interests to disclose.

## Declarations

**Ethics approval** Not applicable

**Consent to publish** Not applicable

**Consent to participate** Not applicable.

**Open Access** This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article’s Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article’s Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

## References

- Aguirre, E., Mahr, D., Grewal, D., de Ruyter, K., & Wetzels, M. (2015). Unraveling the personalization paradox: The effect of information collection and trust-building strategies on online advertisement effectiveness. *Journal of Retailing*, 91(1), 34–49.
- Altay, S., Berriche, M., & Acerbi, A. (2023). Misinformation on misinformation: Conceptual and methodological challenges. *Social Media + Society*, 9(1), 1–13.
- Altay, S., & Acerbi, A. (forthcoming). People believe misinformation is a threat because they assume others are gullible. *New Media & Society*.
- Appel, M., Marker, C., & Gnambs, T. (2020). Are social media ruining our lives? A review of meta-analytic evidence. *Review of General Psychology*, 24(1), 60–74.
- Arceneaux, K., & Johnson, M. (2015). More a Symptom Than a Cause: Polarization and Partisan News Media in America. In J. A. Thurber & A. Yoshinaka (Eds.), *American Gridlock: The Sources, Character, and Impact of Political Polarization* (pp. 309–336). Cambridge University Press.
- Aytac, U. (2024). Digital Domination: Social Media and Contestatory Democracy. *Political Studies*, 72(1), 6–25.

- Bail, C. A., Argyle, L. P., Brown, T. W., Bumpus, J. P., Chen, H., Hunzaker, M. F., & Volfovsky, A. (2018). Exposure to opposing views on social media can increase political polarization. *Proceedings of the National Academy of Sciences*, 115(37), 9216–9221.
- Balebako, R., Leon, P., Shay, R., Ur, B., Wang, Y., & Cranor, L. (2012). *Measuring the effectiveness of privacy tools for limiting behavioral advertising*. Web 2.0 Security and Privacy Workshop.
- Bang, H., Choi, D., Wojdyski, B. W., & Lee, Y. I. (2019). How the level of personalization affects the effectiveness of personalized ad messages: The moderating role of narcissism. *International Journal of Advertising*, 38(8), 1116–1138.
- Barberá, P. (2020). Social media, echo chambers, and political polarization. In N. Persily & J. A. Tucker (Eds.), *Social media and democracy: The state of the field, prospects for reform* (pp. 34–55). Cambridge University Press.
- Barberá, P. (2015). How social media reduces mass political polarization: Evidence from Germany, Spain, and the US. Paper presented at the 2015 American Political Science Association conference.
- Beam, M. A., Hutchens, M. J., & Hmielowski, J. D. (2020). Facebook news and (de) polarization: Reinforcing spirals in the 2016 US election. *Information, Communication & Society*, 21(7), 940–958.
- Benn, C., & Lazar, S. (2022). What's Wrong with Automated Influence. *Canadian Journal of Philosophy*, 52(1), 125–148.
- Biddle, S. (2024). Elon Musk fought government surveillance – while profiting off government surveillance. (<https://theintercept.com/2024/03/25/elon-musk-x-dataminr-surveillance-privacy/>).
- Boerman, S. C., & Smit, E. G. (2023). Advertising and privacy: An overview of past research and a research agenda. *International Journal of Advertising*, 42(1), 60–68.
- Boerman, S. C., Kruikemeier, S., & Zuiderveen Borgesius, F. J. (2017). Online Behavioral Advertising: A Literature Review and Research Agenda. *Journal of Advertising*, 46(3), 363–376.
- Bott, E. (2013). How did mainstream media get the NSA PRISM story so hopelessly wrong? (<https://www.zdnet.com/article/how-did-mainstream-media-get-the-nsa-prism-story-so-hopelessly-wrong/>).
- Boxell, L., Gentzkow, M., & Shapiro, J. M. (2017). Greater Internet use is not associated with faster growth in political polarization among US demographic groups. *Proceedings of the National Academy of Sciences*, 114(40), 10612–10617.
- Braghieri, L., Levy, R. E., & Makarin, A. (2022). Social media and mental health. *American Economic Review*, 112(11), 3660–3693.
- Brailovskaia, J., Ströse, F., Schillack, H., & Margraf, J. (2020). Less Facebook use—More well-being and a healthier lifestyle? An experimental intervention study. *Computers in Human Behavior*, 108(106332), 1–9.
- Braun, S., Flaherty, A., Gillum, J., & Matt Apuzzo. (2013). Secret to Prism program: Even bigger data seizure. What makes Prism work? National Security Agency's megadata collection from Internet pipeline. (<https://www.seattletimes.com/seattle-news/secret-to-prism-program-even-bigger-data-seizure/>).
- Brennan, J. (2014). *Why Not Capitalism?* Routledge.
- Bruns, A. (2019). *Are filter bubbles real?* Polity Press.
- Brynjolfsson, E., Collis, A., & Eggers, F. (2019). Using massive online choice experiments to measure changes in well-being. *Proceedings of the National Academy of Sciences*, 116(15), 7250–7255.
- Burstein, B., Agostino, H., & Greenfield, B. (2019). Suicidal attempts and ideation among children and adolescents in US emergency departments, 2007–2015. *JAMA Pediatrics*, 173(6), 598–600.
- Bursztyn, L., Handel, B. R., Jimenez, R., & Roth, C. (2023). When product markets become collective traps: The case of social media (working paper no. 31771). National Bureau of Economic Research.
- Calo, R. (2013). Digital Market Manipulation. *George Washington Law Review*, 82(4), 995–1051.
- Cambridge Dictionary. Surveillance. (<https://dictionary.cambridge.org/dictionary/english/surveillance>).
- Caplan, B. (2019). Historically Hollow: The Cries of Populism. (<https://www.econlib.org/historically-hollow-the-cries-of-populism>).
- Caplan, B. (2022). The Woke Who Did Not Cancel. (<https://betonit.substack.com/p/the-woke-who-did-not-cancel>).
- Ceci, L. (2022a). Most popular Apple App Store categories as of 3rd quarter 2022, by share of available apps. (<https://www.statista.com/statistics/270291/popular-categories-in-the-app-store>).
- Ceci, L. (2022b). Most popular Google Play app categories as of 3rd quarter 2022, by share of available apps. (<https://www.statista.com/statistics/279286/google-play-android-app-categories>).
- Ceci, L. (2023). Most popular video content type worldwide in 1st quarter 2023, by weekly usage reach (<https://www.statista.com/statistics/1254810/top-video-content-type-by-global-reach>).

- Chomanski, B. (2021). The missing ingredient in the case for regulating big tech. *Minds and Machines*, 31(2), 257–275.
- Claburn, T. (2023). Europe bans Meta from using personal data to target ads: EU folks have no chill, not that we're complaining. ([https://www.theregister.com/2023/11/01/eu\\_data\\_meta\\_networking/](https://www.theregister.com/2023/11/01/eu_data_meta_networking/)).
- Coeckelbergh, M. (2024). *Why AI Undermines Democracy and What to Do About It*. Polity Press.
- Biggest Companies by Market Cap. (<https://stockanalysis.com/list/biggest-companies/>).
- Corrigan, J. R., Alhabash, S., Rousu, M., & Cash, S. B. (2018). How much is social media worth? Estimating the value of Facebook by paying users to stop using it. *PLoS ONE*, 13(12), 1–11.
- Cowen, T. (2019). *Big business: A love letter to an American anti-hero*. St. Martin's Press.
- Dahl, T., Foldnes, N., Grønneberg, S., & Aaen-Stockdale, C. (2024). The risks remain unknown for social media use and adolescent well-being. (<https://osf.io/ycpfh/download>).
- De Keyzer, F., Dens, N., & De Pelsmacker, P. (2022a). How and when personalized advertising leads to brand attitude, click, and WOM intention. *Journal of Advertising*, 51(1), 39–56.
- De Keyzer, F., Van Noort, G., & Kruikeimeier, S. (2022b). Going too far? How consumers respond to personalized advertising from different sources. *Journal of Electronic Commerce Research*, 23(3), 138–159.
- Diakopoulos, N., Trielli, D., Stark, J., & Mussenden, S. (2018). I vote for—how search informs our choice of candidate. In A. Moore & D. Tambini (Eds.), *Digital Dominance: The Power of Google, Amazon, Facebook, and Apple* (pp. 320–342). Oxford University Press.
- Digital Advertising – United States. (<https://www.statista.com/outlook/dmo/digital-advertising/united-states#ad-spending>).
- Eady, G., Paskhalis, T., Zilinsky, J., Bonneau, R., Nagler, J., & Tucker, J. A. (2023). Exposure to the Russian Internet Research Agency foreign influence campaign on Twitter in the 2016 US election and its relationship to attitudes and voting behavior. *Nature Communications*, 14(1), 62.
- Eichenwald, K. (2013). PRISM Isn't Data Mining and Other Falsehoods in the N.S.A. "Scandal". (<https://www.vanityfair.com/news/2013/06/prism-isnt-data-mining-NSA-scandal>).
- Etzioni, A. (2018). Apple: Good business, poor citizen? *Journal of Business Ethics*, 151(1), 1–11.
- Ferguson, C. J., Kaye, L. K., Branley-Bell, D., Markey, P., Ivory, J. D., Klisanin, D., & Wilson, J. (2022). Like this meta-analysis: Screen media and mental health. *Professional Psychology: Research and Practice*, 53(2), 205–214.
- Ferguson, C. J. (forthcoming). Do social media experiments prove a link with mental health: A methodological and meta-analytic review. *Psychology of Popular Media*.
- Fergusson, L., & Molina, C. (2019). Facebook causes protests. *Documento CEDE*(41), 1–107. Fortune 500: Walmart. (<https://fortune.com/company/walmart/fortune500/>)
- Insurance Fraud. (<https://www.fbi.gov/stats-services/publications/insurance-fraud>) Retrieved 09 April, 2024.
- Fukuyama, F. (2011). *The origins of political order: From prehuman times to the French Revolution*. Farrar, Straus and Giroux.
- Fung, B. (2023). FEC dismisses RNC complaint that Google's spam filters were biased against conservatives. (<https://edition.cnn.com/2023/01/18/tech/fec-decision-rnc-gmail-spam/index.html>).
- Garfinkel, B. (2020). The Case for Privacy Optimism. (<https://www.lesswrong.com/posts/4k4FLCPXXdW5cLnvH/the-case-for-privacy-optimism>).
- Gervais, A., Filios, A., Lenders, V., & Capkun, S. (2017). *Quantifying web adblocker privacy*. Paper presented at the Computer Security—ESORICS 2017: 22nd European Symposium on Research in Computer Security, Oslo, Norway, September 11–15, 2017, Proceedings, Part II 22.
- Gezici, G., Lipani, A., Saygin, Y., & Yilmaz, E. (2021). Evaluation metrics for measuring bias in search engine results. *Information Retrieval Journal*, 24, 85–113.
- Gibney, E. (2018). The scant science behind Cambridge Analytica's controversial marketing techniques. *Nature*. (<https://www.nature.com/articles/d41586-018-03880-4>).
- González-Bailón, S., Lazer, D., Barberá, P., Zhang, M., Allcott, H., Brown, T., & Guess, A. M. (2023). Asymmetric ideological segregation in exposure to political news on Facebook. *Science*, 381(6656), 392–398.
- Goujard, C. (2023). Meta's advertising empire faces growing hurdles in Europe: After a new EU court ruling, Facebook and Instagram face renewed pressure over how they gather Europeans' data. (<https://www.politico.eu/article/meta-advertising-empire-faces-growing-hurdles-in-europe/>).
- Guess, A. M., Malhotra, N., Pan, J., Barberá, P., Allcott, H., Brown, T., & Gentzkow, M. (2023). How do social media feed algorithms affect attitudes and behavior in an election campaign? *Science*, 381(6656), 398–404.

- Guess, A. M., Malhotra, N., Pan, J., Barberá, P., Allcott, H., Brown, T., & Gentzkow, M. (2023). Reshares on social media amplify political news but do not detectably affect beliefs or opinions. *Science*, 381(6656), 404–408.
- Guo, B., & Jiang, Z. B. (forthcoming). Influence of personalised advertising copy on consumer engagement: A field experiment approach. *Electronic Commerce Research*, 1–30.
- Gupta, S. (2020). Encryption - Big-Tech vs The Government. (<https://medium.com/dataseries/encryption-big-tech-vs-government-6b3c853edc41>).
- Gustin, S. (2013). AT&T and Verizon Stay Silent About NSA Internet Snooping: The telecom giants don't have much to say about their role in NSA surveillance programs. *Time*. (<https://business.time.com/2013/08/22/att-and-verizon-stay-silent-about-nsa-internet-snooping/>).
- Haidt, J., Rausch, Z., & Twenge, J. (ongoing). Social media and mental health: A collaborative review. Unpublished manuscript, New York University. ([tinyurl.com/SocialMediaMentalHealthReview](https://tinyurl.com/SocialMediaMentalHealthReview)).
- Haidt, J., Rausch, Z., & Twenge, J. (ongoing). Adolescent mood disorders since 2010: A collaborative review. Unpublished manuscript, New York University. ([https://docs.google.com/document/d/1diMvsMeRphUH7E6D1d\\_J7R6WbDdgnzFHDHPx9HXzR5o](https://docs.google.com/document/d/1diMvsMeRphUH7E6D1d_J7R6WbDdgnzFHDHPx9HXzR5o)).
- Harvard Law Review Staff. (2018). Developments in the Law – More Data. *More Problems. Harvard Law Review*, 131(6), 1714–1811.
- Heilweil, R. (2020). Big tech companies back away from selling facial recognition to police. That's progress. After IBM, Amazon, and Microsoft upend their facial recognition businesses, attention turns to federal lawmakers. (<https://www.vox.com/recode/2020/6/10/21287194/amazon-microsoft-ibm-facial-recognition-moratorium-police>).
- Hoeksema, B. (2023). Digital Domination and the Promise of Radical Republicanism. *Philosophy & Technology*, 36(1), 17.
- Holpuch, A. (2016). Tim Cook says Apple's refusal to unlock iPhone for FBI is a 'civil liberties' issue. (<https://www.theguardian.com/technology/2016/feb/22/tim-cook-apple-refusal-unlock-iphone-fbi-civil-liberties>).
- Hoye, J. M., & Monaghan, J. (2018). Surveillance, freedom and the republic. *European Journal of Political Theory*, 17(3), 343–363.
- Huszár, F., Ktena, S. I., O'Brien, C., Belli, L., Schlaikjer, A., & Hardt, M. (2022). Algorithmic amplification of politics on Twitter. *Proceedings of the National Academy of Sciences*, 119(1), 1–6.
- Ibrahim, H., AlDahoul, N., Lee, S., Rahwan, T., & Zaki, Y. (2023). YouTube's recommendation algorithm is left-leaning in the United States. *PNAS Nexus*, 2(8), 1–9.
- Ireland, S. (2021). Cooperation or Resistance? How Big Tech Handles Data Requests from Governments. (<https://ceoworld.biz/2021/11/24/cooperation-or-resistance-how-big-tech-handles-data-requests-from-governments/>).
- Izant, C. L. (2017). Equal Access to Public Communications Data for Social Media Surveillance Software. *Harvard Journal of Law & Technology*, 31(1), 237–257.
- Jiang, S., Robertson, R. E., & Wilson, C. (2020). Reasoning About Political Bias in Content Moderation. *Paper presented at the Proceedings of the AAAI Conference on Artificial Intelligence*, 34, 9.
- Johnston, M. (2023). How Does Facebook (Meta) Make Money?. (<https://www.investopedia.com/ask/answers/120114/how-does-facebook-fb-make-money.asp>).
- Jost, J. T., Barberá, P., Bonneau, R., Langer, M., Metzger, M., Nagler, J., & Tucker, J. A. (2018). How social media facilitates political protest: Information, motivation, and social networks. *Political Psychology*, 39(Suppl. 1), 85–118.
- Karpf, D. (2019). On Digital Disinformation and Democratic Myths. (<https://mediawell.ssrc.org/articles/on-digital-disinformation-and-democratic-myths/>).
- Keyes, K. M., Gary, D., O'Malley, P. M., Hamilton, A., & Schulenberg, J. (2019). Recent increases in depressive symptoms among US adolescents: Trends from 1991 to 2018. *Social Psychiatry and Psychiatric Epidemiology*, 54(8), 987–996.
- Kim, J. J., Kim, T., Wojdyski, B. W., & Jun, H. (2022). Getting a little too personal? Positive and negative effects of personalized advertising on online multitaskers. *Telematics and Informatics*, 71, 101831.
- Kircher, T., & Foerderer, J. (2024). Ban Targeted Advertising? An Empirical Investigation of the Consequences for App Development. *Management Science*, 70(2), 1070–1092.
- Königs, P. (2022). Government Surveillance, Privacy, and Legitimacy. *Philosophy & Technology*, 35, 8.
- Kubin, E., & von Sikorski, C. (2020). The role of (social) media in political polarization: A systematic review. *Annals of the International Communication Association*, 45(3), 188–206.

- Kulshrestha, J., Eslami, M., Messias, J., Zafar, M. B., Ghosh, S., Gummadi, K. P., & Karahalios, K. (2019). Search bias quantification: Investigating political bias in social media and web search. *Information Retrieval Journal*, 22, 188–227.
- Kupferschmidt, K. (2023). Studies find little impact of social media on polarization. *Science*, 381(6656), 367–368.
- Lambrecht, A., & Tucker, C. (2013). When does retargeting work? Information specificity in online advertising. *Journal of Marketing Research*, 50(5), 561–576.
- Largest Companies by Market Cap. (<https://companiesmarketcap.com/twitter/marketcap/>)
- Lawford-Smith, H. (2022). Ending Discrimination by Twitter: Gender critical feminists are among those who have been excluded from Twitter for years. The time is right for a correction. (<https://quillette.com/2022/11/28/ending-discrimination-on-twitter/>)
- Lutz, M., Gadaginmath, S., Vairavan, N., & Mui, P. (2021). Examining political bias within YouTube search and recommendation algorithms. In *2021 IEEE Symposium Series on Computational Intelligence (SSCI)* (pp. 1–7). IEEE.
- Lyon, D. (2001). *Surveillance Society: Monitoring Everyday Life*. Open University Press.
- Macnish, K. (2018a). *The Ethics of Surveillance: An Introduction*. Routledge.
- Macnish, K. (2018b). Government Surveillance and Why Defining Privacy Matters in a Post-Snowden World. *Journal of Applied Philosophy*, 35(2), 417–432.
- Macnish, K. (2020). Mass surveillance: A private affair? *Moral Philosophy and Politics*, 7(1), 9–27.
- McCloskey, D. (2019). *Why Liberalism Works: How True Liberal Values Produce a Freer, More Equal, Prosperous World for All*. Yale University Press.
- McQuade III, S. C., & Danielson, P. (2005). Monitoring and Surveillance. In C. Mitcham (Ed.), *Encyclopedia of Science and Technology Ethics: Volume 3* (pp. 1228–1232). Detroit: Thomson Gale.
- Meaker, M. (2023a). Facebook Finally Puts a Price on Privacy: It's \$10 a Month. (<https://www.wired.com/story/meta-facebook-pay-for-privacy-europe/>).
- Meaker, M. (2023b). The Slow Death of Surveillance Capitalism Has Begun: A European Union ruling against Meta marks the beginning of the end of targeted ads. (<https://www.wired.co.uk/article/meta-surveillance-capitalism>).
- Meier, A., & Reinecke, L. (2021). Computer-mediated communication, social media, and mental health: A conceptual and empirical meta-review. *Communication Research*, 48(8), 1182–1209.
- Mejias, U. A., & Couldry, N. (2024). *Data Grab: The New Colonialism of Big Tech and How to Fight Back*. University of Chicago Press.
- Menges, L. (2020). Did the NSA and GCHQ diminish our privacy? What the control account should say. *Moral Philosophy and Politics*, 7(1), 29–48.
- Le Merrer, E., Morgan, B., & Trédan, G. (2021). Setting the record straighter on shadow banning. Paper presented at the IEEE INFOCOM 2021-IEEE Conference on Computer Communications.
- Merzdownik, G., Huber, M., Buhov, D., Nikiforakis, N., Neuner, S., Schmiedecker, M., & Weippl, E. (2017). *Block me if you can: A large-scale study of tracker-blocking tools*. Paper presented at the 2017 IEEE European Symposium on Security and Privacy.
- Molla, R. (2018). Tech employees are much more liberal than their employers — at least as far as the candidates they support. (<https://www.vox.com/2018/10/31/18039528/tech-employees-politics-liberal-employers-candidates>).
- Moore, A. (2008). Defining Privacy. *Journal of Social Philosophy*, 39(3), 411–428.
- Morrison, S. (2020). Why Attorney General Bill Barr is mad at Apple: The FBI didn't need Apple's help to crack a suspected terrorist's iPhone, but it's demanding it anyway. (<https://www.vox.com/recode/2020/5/18/21262731/fbi-apple-unlock-iphone-encryption-bill-barr-alshamrani>).
- Mosleh, M., Yang, Q., Zaman, T., Pennycook, G., & Rand, D. G. (MS). Trade-offs between reducing misinformation and politically-balanced enforcement on social media.
- Nechushtai, E., Zamith, R., & Lewis, S. C. (forthcoming). More of the Same? Homogenization in News Recommendations When Users Search on Google, YouTube, Facebook, and Twitter. *Mass Communication and Society*.
- Norberg, J. (2023). *The Capitalist Manifesto: Why the Global Free Market Will Save the World*. Atlantic Books.
- Nyhan, B., Settle, J., Thorson, E., Wojcieszak, M., Barberá, P., Chen, A. Y., & Dimmery, D. (2023). Like-minded sources on Facebook are prevalent but not polarizing. *Nature*, 620(7972), 137–144.
- O'Toole, L. (2021). Are Google search results biased? (<https://www.authoritas.com/blog/are-google-search-results-biased>)

- Odgers, C. L. (2024). The great rewiring, unplugged. Is social media really behind an epidemic of teenage mental illness? *Nature*, 628(8006), 29–30.
- Odgers, C. L., & Jensen, M. R. (2020). Annual research review: Adolescent mental health in the digital age: Facts, fears, and future directions. *Journal of Child Psychology and Psychiatry*, 61(3), 336–348.
- Oldenbourg, A. (2024). Digital freedom and corporate power in social media. *Critical Review of International Social and Political Philosophy*, 27(3), 383–404.
- Orben, A. (2020). The Sisyphean cycle of technology panics. *Perspectives on Psychological Science*, 15(5), 1143–1157.
- Pettit, P. (2014). *On the People's Terms: A Republican Theory and Model of Democracy*. Cambridge University Press.
- Raz, J. (1988). Autonomy, Toleration, and the Harm Principle. In S. Mendus (Ed.), *Justifying Toleration: Conceptual and Historical Perspectives* (pp. 155–175). Cambridge University Press.
- Risse, M. (2023). *Political Theory of the Digital Age: Where Artificial Intelligence Might Take Us*. Cambridge University Press.
- Roberts, A. (2015). A republican account of the value of privacy. *European Journal of Political Theory*, 14(4), 320–344.
- Robertson, R. E., Jiang, S., Joseph, K., Friedland, L., Lazer, D., & Wilson, C. (2018). Auditing partisan audience bias within google search. *Proceedings of the ACM on Human-Computer Interaction*, 2(CSCW), 1–22.
- Ross Arguedas, A., Robertson, C., Fletcher, R., & Nielsen, R. (2022). Echo chambers, filter bubbles, and polarisation: A literature review. Reuters Institute for the Study of Journalism. (<https://reutersinstitute.politics.ox.ac.uk/echo-chambers-filter-bubbles-and-polarisation-literature-review>).
- Rozenshtein, A. Z. (2018). Surveillance Intermediaries. *Stanford Law Review*, 70(1), 99–189.
- Savage, C. (2017). *Power Wars: The Relentless Rise of Presidential Authority and Secrecy*. Back Bay Books.
- Seele, P., Dierksmeier, C., Hofstetter, R., & Schultz, M. D. (2021). Mapping the ethicality of algorithmic pricing: A review of dynamic and personalized pricing. *Journal of Business Ethics*, 170(4), 697–719.
- Settle, J. E. (2018). *Frenemies: How Social Media Polarizes America*. Cambridge University Press.
- Soave, R. (2021). *Tech Panic: Why We Shouldn't Fear Facebook and the Future*. Simon and Schuster.
- Solon, O. (2017). Facebook among tech firms battling gag orders over government surveillance. (<https://www.theguardian.com/technology/2017/jul/10/facebook-twitter-surveillance-gag-order>).
- Sorell, T. (2018). Bulk collection, intrusion and domination. In A. I. Cohen (Ed.), *Philosophy and Public Policy* (pp. 39–60). Rowman & Littlefield.
- Spencer, S. B. (2020). The problem of online manipulation. *University of Illinois Law Review*, 2020(3), 959–1006.
- Srnicek, N. (2017). *Platform Capitalism*. Cambridge, UK: Polity.
- Stahl, T. (2016). Indiscriminate mass surveillance and the public sphere. *Ethics and Information Technology*, 18(1), 33–39.
- Stein, C. (2023). Stanford professor put on Twitter's 'Trends Blacklist'. (<https://stanforddaily.com/2023/01/18/stanford-professor-put-on-twiters-trends-blacklist/>).
- Steinberg, E. (2022). Run for your life: The ethics of behavioral tracking in insurance. *Journal of Business Ethics*, 179(3), 665–682.
- Steinert-Threlkeld, Z. C., Mocanu, D., Vespignani, A., & Fowler, J. (2015). Online social networks and offline protest. *EPJ Data Science*, 4(1), 1–9.
- Sunstein, C. (2018). *#Republic: Divided democracy in the age of social media*. Princeton University Press.
- Susser, D., Roessler, B., & Nissenbaum, H. (2019a). Online manipulation: Hidden influences in a digital world. *Georgetown Law Technology Review*, 4(1), 1–45.
- Susser, D., Roessler, B., & Nissenbaum, H. (2019b). Technology, autonomy, and manipulation. *Internet Policy Review*, 8(2), 1–22.
- Taylor, L. (2021). Public actors without public values: Legitimacy, domination and the regulation of the technology sector. *Philosophy & Technology*, 34(4), 897–922.
- Tran, T. P., Lin, C. W., Baalbaki, S., & Guzmán, F. (2020). How personalized advertising affects equity of brands advertised on Facebook? A mediation mechanism. *Journal of Business Research*, 120, 1–15.

- Tucker, J. A., Guess, A., Barberá, P., Vaccari, C., Siegel, A., Sanovich, S., & Nyhan, B. (2018). Social media, political polarization, and political disinformation: A review of the scientific literature. Political polarization, and political disinformation: a review of the scientific literature. Hewlett Foundation.
- Twenge, J. M. (2020). Why increases in adolescent depression may be linked to the technological environment. *Current Opinion in Psychology*, 32, 89–94.
- Twenge, J. M. (2023). *Generations: The Real Differences Between Gen Z, Millennials, Gen X, Boomers, and Silents – and What They Mean for America's Future*. Simon and Schuster.
- Twenge, J. M., Cooper, A. B., Joiner, T. E., Duffy, M. E., & Binau, S. G. (2019). Age, period, and cohort trends in mood disorder indicators and suicide-related outcomes in a nationally representative dataset, 2005–2017. *Journal of Abnormal Psychology*, 128(3), 185–199.
- Vaidhyathan, S. (2018). *Antisocial media: How Facebook disconnects us and undermines democracy*. Oxford University Press.
- Valkenburg, P. M. (2022). Social media use and well-being: What we know and what we need to know. *Current Opinion in Psychology*, 45(101294), 1–8.
- Valkenburg, P. M., Meier, A., & Beyens, I. (2022). Social media use and its impact on adolescent mental health: An umbrella review of the evidence. *Current Opinion in Psychology*, 44, 58–68.
- Varian, H. R. (2014). Beyond Big Data. *Business Economics*, 49(1), 27–31.
- Varnali, K. (2021). Online behavioral advertising: An integrative review. *Journal of Marketing Communications*, 27(1), 93–114.
- Véliz, C. (2020). *Privacy Is Power: Why and How You Should Take Back Control of Your Data*. Bantam Press.
- Venkatesh, N. (2021). Surveillance Capitalism: A Marx-inspired account. *Philosophy*, 96(3), 359–385.
- Victory: U.S. won't try to gag Facebook from telling users about warrants for their data. (2017). (<https://www.accessnow.org/press-release/victory-u-s-wont-try-gag-facebook-telling-users-warrants-data/>).
- Vinsel, L. (2021). You're Doing It Wrong: Notes on Criticism and Technology Hype. (<https://sts-news.medium.com/youre-ng-it-wrong-notes-on-criticism-and-technology-hype-18b08b4307e5>).
- Waterson, J. (2020). Cambridge Analytica did not misuse data in EU referendum, says watchdog. (<https://www.theguardian.com/uk-news/2020/oct/07/cambridge-analytica-did-not-misuse-data-in-eu-referendum-says-watchdog>).
- Williams, A., & Raekstad, P. (2022). Surveillance Capitalism or Information Republic? *Journal of Applied Philosophy*, 39(3), 421–440.
- Winter, S., Maslowska, E., & Vos, A. L. (2021). The effects of trait-based personalization in social media advertising. *Computers in Human Behavior*, 114, 106525.
- Wyatt, E., & Miller, C. C. (2013). Tech Giants Issue Call for Limits on Government Surveillance of Users. *The New York Times*. (<https://www.nytimes.com/2013/12/09/technology/tech-giants-issue-call-for-limits-on-government-surveillance-of-users.html>).
- Zak, P. J., & Knack, S. (2001). *Trust and Growth*. *the Economic Journal*, 111(470), 295–321.
- Zuboff, S. (2015). 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*. Profile Books.
- Zuboff, S. (2022). Surveillance Capitalism or Democracy? The Death Match of Institutional Orders and the Politics of Knowledge in Our Information Civilization. *Organization Theory*, 3(3), 1–79.
- ZuiderveenBorgesius, F., Trilling, D., Möller, J., Bodó, B., De Vreese, C. H., & Helberger, N. (2016). Should we worry about filter bubbles? *Internet Policy Review*, 5, 1.