

Mostly Harmless? Everyday Smart Speaker Use and Pragmatic Fatalism

David Waldecker, Alexander Martin, and Dagmar Hoffmann

Abstract Breaches of trust and privacy by tech companies and the ensuing scandals emphasize how today's digital media are driven by the monetization of users' personal data. Studies of users' attitudes to data protection issues in connection with the use of digital media technologies have led researchers to conclude that users develop a kind of "online apathy" (Hargittai and Marwick 2016), "privacy cynicism" (Hoffmann et al. 2016) or "digital resignation" (Draper and Turow 2019). This chapter examines users' experiences of smart speakers in daily life and their understandings of the data-related consequences of their everyday use of the devices. We draw upon qualitative interviews conducted with smart speaker users in Germany to illustrate how they cultivate certain attitudes towards the devices as well as to the discourse about them, and how they explain their stances in relation to usage routines and pragmatic considerations. While our interviewees asserted views similar to some described by the aforementioned researchers, in this chapter we argue that the attitudes expressed by smart speaker users can be better understood as "pragmatic fatalism" (Pettenkofer 2017). Pragmatic fatalism allows them to acknowledge criticism of corporate data practices yet disregard it as irrelevant for their own everyday lives. The perceived harmlessness of devices, usage practices, and users themselves is emphasized as justification for not worrying about the potential consequences of bringing technology that constantly records interactions into one's own home.

1. Introduction

In modern societies, the home is seen as a private space *par excellence*. Laws that guarantee homeowners and sometimes tenants extensive control over their living spaces also cover the control over information relating to the home. The value attributed to privacy by German citizens was testified to in the late 20th

century when a debate about privacy and data protection was sparked by activists who fought for the individual's right to not be included in a census survey (Lengwiler 2017, 6). One can argue that that notorious debate continues to shape German, and consequently, European data protection laws to this day. The issue of domestic data protection has also been raised in relation to smart speakers, also known as intelligent personal assistants (IPAs). Available since 2014, these devices promise comfort and access to smart home and internet services by voice activation alone – without the push of a button. In order to be able to respond when a command is uttered, they need to constantly record the ambient sounds of the home. This technical setup, in combination with the awareness that the platform companies that offer such devices are known to harvest and analyze data, has led to critiques that condemn a hollowing out of domestic privacy and even “remote control” of home dwellers by these companies (Zuboff 2020).

In this contribution, we examine smart speaker users' understandings, strategies and perspectives on this potential for commercial misuse of the data produced in smart speaker use. Research on privacy issues related to digitally-connected media practices has found that users cultivate a form of “online apathy” (Hargittai and Marwick 2016), “privacy cynicism” (Hoffmann et al. 2016) or “digital resignation” (Draper and Turow 2019). We revisit this debate with a focus on pragmatic aspects and a pragmatistic theoretical conceptualization of users' behavior (see Pettenkofer 2017; 2023) to offer a complementary interpretation. We relate this theoretical discussion to findings from problem-centered interviews conducted as part of our research project “Un-/desired Observation in Interaction: ‘Intelligent Personal Assistants’ (IPAs)” at the Collaborative Research Center “Media of Cooperation”, University of Siegen, from 2020 to 2023 (see Habscheid et al., this volume).

This chapter proceeds as follows: After reviewing literature on users' perspectives on online privacy, we propose the need for a more pragmatic and supra-individual approach. With this in mind, we also discuss the domestication perspective on media and information and communication technologies (ICTs) as well as social theory that focuses on the role of fatalism in everyday life (Pettenkofer 2023). Our sampling and methods are detailed in the following section. Subsequently, we present key elements of our empirical analysis and we close with a discussion of the findings and their relevance for further debate on online media and data practices.

2. From Privacy Paradox to Privacy Cynicism

With the advent of everyday online interaction and services, privacy as it is commonly understood has been seen to come under threat, (1) from corporate and state surveillance, i.e., organizational surveillance, and (2) from surveillance by other online users.

(1) The majority of online services are provided by private companies with an economic imperative (Kienscherf, this volume). An easy way to monetize free-to-use services is by selling advertising space. One of the first companies to undertake online corporate surveillance was Google (Zuboff 2019): by analyzing users' reactions to results from its search engine, Google was able to build user profiles so that it could place online ads most likely to align with users' interests. This strategy has been adopted by almost all providers of commercial online services. Online stores as well as newspaper websites analyze how users interact with their platforms so that they can adapt the content presented accordingly in order to maximize advertising effectivity and user engagement. The more information companies have about their users, the better positioned they are to judge which ads are likely to resonate. This is what created the drive towards big data that is prevalent today. Alongside hardware and software manufacturers like Apple and Microsoft, the main profits of companies like Meta/Facebook and Google are generated from online advertising. As critics like Zuboff suggest, the vast amounts of data collected not only allow companies to place targeted ads, but also to influence user behavior for companies' financial gain (Zuboff 2020). While the field of surveillance studies is informed by critiques of data use by state agencies for surveillance and control, it was also early to draw attention to the aforementioned corporate tracking of consumers and media users (Gandy, 1989)¹. These corporate practices have been with us since the late 19th century (Lauer 2020). Hence, the corporate analysis of data obtained from smart speaker use should be understood not as a novel phenomenon but as a continuation or further development of earlier forms of corporate surveillance and indirect market research (Draper and Turow 2019, Kienscherf this volume).

(2) The last two decades have witnessed not only a rapid commercialization, platformization, and oligopolization of online services, but also the rise of personal publishing (see e.g., Taddicken and Schmidt 2016) by online users

1 Note that Gandy already used the term "surveillance society" 20 years before Zuboff did (2019).

via social media. Beginning with MySpace (2003) and Facebook (2004) in the United States and StudiVZ (2005) in Germany, users of the so-called Web 2.0 (O'Reilly 2012) were suddenly able to create content and disseminate it online without needing skills in computer programming or markup language. Activities formerly associated with the private sphere were made visible online and thereby became public affairs, of sorts.

In debates on threats to privacy, it is this use of social media that has often been invoked with the idea of the “privacy paradox” (Barnes 2006; Norberg et al. 2007). The term describes the paradox of a high value attributed to online privacy in co-occurrence with actions that imply disregarding such privacy. While early research put the paradox down to the two-fold inexperience of young users and of a new and interconnected medium (Barnes 2006), later work has tried to disentangle the paradox in other ways (boyd 2014). It seems that, over time, users became better informed about online data practices, but also came to see them as inevitable, leading to what Hargittai and Marwick (2016) term “online apathy.” In their research, young users reported that they were informed about the risks of exposing information about themselves online but felt simultaneously pressurized by peers to do so. Here, the paradox was no longer about contradictory “sayings” and “doings” (cf., e.g., Kahn and Jeromack, 2013) – claiming to cherish privacy, but acting otherwise –, but resulted from conflicting imperatives from school, parents, and peers concerning social media. Research conducted at our research center in Germany also suggests that young adults know and care about interpersonal online privacy and therefore consider carefully what kinds of personal content to post on platforms such as Instagram (cf. Englert et al., 2019). Teens interviewed in our study, however, mentioned that they used social media less for personal presentation than for staying up to date on posted content².

In addition to conflicting imperatives concerning privacy and publicity of online lives, Draper and Turow (2019) note how “digital resignation” regarding privacy is also fostered and “cultivated” by online corporations. Corporations employ “obfuscatory communication practices” (Draper and Turow, 2019, 1830) that make it hard for individuals to obtain precise information about the use

2 In addition, such conflict between imperatives to uphold privacy yet also to present oneself publicly on social media platforms has become less prevalent since certain forms of interaction shifted from platforms that are public by default (such as Facebook and Instagram) to messenger apps that are private by default (such as WhatsApp, Signal, and Telegram).

of their data. This, in turn, creates a feeling of “resignation” in users who feel unable to change or clarify details about the use of their private data by corporations. Draper and Turow highlight how “feelings of resignation are a rational emotional response in the face of undesirable situations that individuals believe they cannot combat” (Draper and Turow, 2019, 1828). Here, again, it is the way the technical infrastructure is organized and advertised by corporations – shaping the social situation of users – which is seen to determine users’ privacy practices.

This resignation has also, we suggest, been fostered by a shifting media narrative about online corporations. Internet researcher and activist Geert Lovink (2019) has noted how early hopes and enthusiasm for cyberspace gave way to a more dystopian and critical view of a web dominated by corporations and advertisement. The revelations by Edward Snowden concerning online surveillance, and scandals such as Facebook’s involvement with online elections ads via Cambridge Analytica, combined with a tougher policy approach to corporate data use, have all helped to propagate views that criticize corporate data handling and denounce privacy violations. This perspective on privacy violations is especially pertinent to voice assistants because in VA use users do not primarily interact with other users, but with a synthetic agent provided by a company.

The resignation and apathy discussed above has also been addressed with specific reference to users of voice assistants. In several publications, Christoph Lutz (Lutz and Strahoff, 2014; Lutz and Newlands, 2021), Christian Hoffmann, and Giulia Rancini (Hoffmann, Lutz and Rancini, 2016; 2020) have proposed the concept of “privacy cynicism”. Whereas Draper and Turow (2019) emphasize the consequences of corporate strategies, the term “cynicism” conveys not just a feeling that attempting to take action would be futile, but also implies negative views towards an antagonist:

As such, we understand privacy cynicism as an attitude of uncertainty, powerlessness, and mistrust toward the handling of personal data by digital platforms, rendering privacy protection subjectively futile ... In this context of ubiquitous institutional privacy threats, privacy cynicism can be understood as a cognitive coping mechanism because it allows subjectively disempowered users to participate in online platforms without cognitive dissonance since they rationalize privacy protection as useless. (Lutz, Hoffmann and Rancini, 2020, 1174)

Lutz, Hoffmann and Rancini developed their concept based on the findings of a large-scale survey on online privacy and data protection conducted in Germany (*ibid.*). The investigation focused on forms of data handling by online services in general (not related to specific services or devices) that make attempts to protect privacy appear futile. The authors empirically differentiated four aspects of cynicism – mistrust, uncertainty, powerlessness, and resignation (1178) – and examined how they related to users' internet skills, privacy concerns, privacy threat experience, and privacy protection behavior (1181).

The contributions mentioned above have advanced and nuanced understanding of users' actions and perspectives relating to data and privacy in a world of interconnected devices and services. They have shown that the privacy paradox is not primarily a psychological problem or one of motivation or lack of information (about safer or alternative information and communication technologies (ICTs)), but is related to the ways that data collection is inextricably built into digital platforms and services as well as to the ways in which these services have become an integral part of the indispensable social infrastructure of everyday life.

While these explanations can be understood as strongly contextualized approaches – they analyze more than just the perceptions and actions of individuals – they nonetheless focus on individualized fatalistic perspectives. Conceptually, studies in this field rarely take into account that people discuss their use of ICTs with peers, friends, and household members. We therefore propose that further insights can be gained by drawing on the domestication approach in media studies which examines how new ICTs are adopted and used in households and other organizational units. In a foundational text, Roger Silverstone, Eric Hirsch, and David Morley (1992, 12) conceptualize the ways a household uses ICTs as part of its “moral economy”: Users collectively evaluate media devices and services with respect to domestic routines and normative expectations, as well as financial, spatial, and time constraints. The organization of domestic everyday life can be understood as a complex of normative and economic decisions that come together in practice. Taking up the metaphor of the domestication of animals by humans, this perspective describes how users collectively adopt and domesticate media to their specific needs, as well as how their daily lives are changed through media use, sometimes in unexpected ways. Recent research has applied these ideas to the study of modern and interconnected ICTs (Hector et al., 2023). This includes research which looks at the “externalisation” (Brause and Blank, 2020) of domestic tasks through smart home infrastructure – which in turn is often

controlled via domestic voice assistants (cf. Strüver 2023). This approach is well suited to studying domestic voice assistants and connected smart speakers, which are designed to be used by multiple users (unlike smartphones and smart watches). Here, the household is all the more relevant because its domestic space is surveilled via these devices and the devices can, in turn, be addressed by anyone in the space.

Alongside this empirical addition, we respond to the call of Lutz and his colleagues (Lutz, Hoffmann and Ranzini 2020, 1173) for further theoretical elaboration of what is meant by apathy, resignation, or fatalism. While Lutz and colleagues, like Draper and Turow (2019), draw on previous explications of cynicism and resignation respectively, we choose *fatalism* as a term to describe user perspectives and behavior. As Andreas Pettenkofer points out (2017, 2023), fatalism has been a topic in social theory since the latter's inception. Although fatalism is usually perceived as a negative trait – as an acquiescence to one's supposed fate, and thus, an attitude that inhibits action – Pettenkofer highlights ways in which fatalism is positively related to agency. From a pragmatic perspective, deciding not to think about a problem can create new possibilities for action by freeing the individual from the need to deal with the problem or its potential consequences (Pettenkofer 2017, 131). In this way, fatalism as a concept is also able to describe how users actively cope with their inability to change the data-harvesting infrastructures of many digital services. Lutz and colleagues (2020, 1173) conclude that users deal with these aspects of digital services by grudgingly accepting them as inevitable. In Pettenkofer's discussion, however, fatalism is discussed in greater depth. He argues that fatalism is a phenomenon not only among the disadvantaged, who have to accept their situation because they only have limited options for action, but that it comes in multiple shapes and sizes. For the middle class, fatalism can be part of positive thinking and for the upper or executive class, it can represent the recurrent choice not to think through the social and ecological consequences of their economic or political decisions, for example. As such, Pettenkofer argues, fatalism is not an exception to the rational and action-oriented outlook that is often perceived to be a cornerstone of the modern subject, but far more widespread than is often acknowledged in social theory.

Pettenkofer emphasizes (2017, 130 [our translation]) that “fatalism is ... not simply a perception of limits to action, but a pattern of reflection that *emerges* from a specific perception of such limits”. Fatalism relieves us from thinking and thereby makes us capable of acting and has the effect of upholding order. Furthermore, it is important that fatalistic patterns of interpretation are based

on everyday attitudes and experiences that make it easy to publicly justify a lack of alternatives. Pettenkofer differentiates three constellations that can lead to a decision to stop reflecting (2017, 130–132): (1) Conceivable alternatives are or have become too abstract or too far removed from the individual's situation to be worthy of consideration; (2) the participants stop thinking about the application of certain evaluation criteria when justification and criticism have no consequences; (3) the participants give up trying to understand or resist the fateful process because it is too complex or because such action seems futile.

As Pettenkofer (2017) also sees positive thinking as part of this fatalistic mindset, his theoretical perspective can help to situate voice assistant users' critique and their perceived inaction. Characterizing user perspectives with terms such as "apathy", "resignation", and "cynicism" might imply that users are severely affected by their potential loss of privacy. As we elaborate in this chapter, we consider it significant that some users criticize corporate data practices yet do not seem so concerned that they stop using smart speakers. While fatalism has negative connotations such as resignation, the following elaboration will show how we conceptualize users' nonchalance despite concerns, with reference to Pettenkofer's understanding of the term.

In the following, we examine the (fatalistic) patterns of reflection that emerged in our interviews. We adopt Pettenkofer's differentiation of "re-signed" versus "pragmatic fatalism" (Pettenkofer 2017, 143) to explore results from our empirical data and argue that Pettenkofer's concept of fatalism offers a useful aid for analysis of everyday data practices in smart speaker use.

3. Research Design

Our analysis is based on data generated in our research on smart speakers which examined interaction between users, devices, infrastructure, and language from a linguistic and media-sociological perspective. This chapter focuses on the media-sociological aspects of the research and data (see the introduction to this volume for a presentation of the research project and Habscheid, Hector, and Hrnkal, this volume, for a more detailed presentation of the linguistic strand of the project).

Table 1: Sample

Household	Pseudonym	Age	Gender	Number and Type of IPAs	No. of Inter-views	Duration Intv. 1	Duration Intv. 2
1	Lukas F.	25	m	2 Amazon Echo Dot	2	00:55:14	01:05:48
1	Alex K.	27	m	2 Amazon Echo Dot	2	01:12:54	01:38:05
2	Jan-Ole S.	25	m	1 Amazon Echo Dot	2	00:45:05	01:33:56
2	Damaris L.	24	f	1 Amazon Echo Dot	2	00:47:30	01:42:09
3	Beate W.	61	f	1 Google Nest	2	00:58:56	01:14:15
4	Sam R.	27	m	1 Amazon Echo Dot	1	-	01:26:07
4	Andrea S.	25	f	1 Amazon Echo Dot	1	-	02:43:42
5	Julian R.	42	m	4 Apple Home Pod	1	-	01:59:13
6	Alexander R.	31	m	1 Apple Home Pod	1	-	01:10:56
6	Janina R.	29	f	1 Apple Home Pod	1	-	00:56:41
7	Till W.	21	m	1 Amazon Echo, 1 Apple Home Pod	2	01:15:48	01:23:08
7	Konrad W.	21	m	1 Amazon Echo, 1 Apple Home Pod	2	01:09:39	00:48:25
8	Samuel M.	30	m	1 Google Nest, 1 Amazon Echo	2	00:57:57	01:14:24
8	Robin L.	24	m	1 Google Nest	2	00:50:37	-
8	Lara S.	24	f	1 Google Nest, 1 Amazon Echo Dot	1	00:36:55	-
E	Dilek U.	26	f	1 Google Nest, 1 Amazon Echo	1	-	00:47:43
F	Tobias G.	42	m	1 Apple Home Pod, 1 Amazon Echo	1	-	00:56:21
G	Mukesh V.	26	m	1 Amazon Echo	1	-	01:15:10
H	Stefanie L.	34	f	1 Amazon Echo Dot	1	-	00:51:00

The goal was not only to observe and record dialogues of users and their IPA infrastructures, but also to examine users' perspectives and reflections upon IPA usage, on privacy concerns, and ways to deal with them. 28 interviews were conducted with 19 interlocutors in twelve households. Nine of the participants were interviewed twice: first, when they had just set up their newly acquired smart speaker, and then again a few months later.

As shown in the table of participants, most of the households in our sample had one or two IPAs. Amazon's Echo was used by the majority of households, followed by Apple's Home Pod. Google Nest was used in two households. The frequency of usage and technological skills of the participants varied widely. While most simply used their devices without connecting them to other hardware and without much interest in investigating further capabilities, some displayed a higher level of skill and interest (e.g., by connecting additional devices). Most participants lived in multi-person households. Our sample included different living constellations: cohabiting couples, shared apartments, and family households. When we could interview several members of the same household, we were able to take the relationships between their members into account. Friends or other family members play an important role in these constellations. In one case, an interviewee's fiancée lived abroad, making mediated communication essential for sustaining the relationship. The majority of the interviews were held in German, with one conducted in English. At the time of the survey, the respondents were aged between 20 and 60 years old and all had a relatively high level of education. Due to the COVID-19 pandemic, we were unable to visit participants in their homes. Interviews were therefore conducted remotely via the video conferencing tools Jitsi or Big Blue Button.

Problem-centered interviews (Witzel and Reiter, 2012) were carried out with all participants. This form of interview was chosen in order to (a) focus less on biographical narratives and more on a specific aspect of social life and (b) allow for a more direct confrontation of interviewees with discrepancies and ambiguous statements in their reports than other qualitative interviews methods would. The interviews also included show-and-tell episodes wherein interviewer and interviewee looked and listened together at the audio recordings of interactions provided by Amazon and Google to its users. These sessions facilitated further discussion of the companies' mode of data presentation, protection, and transparency.

The interviews were transcribed and all personal information pseudonymized. The transcripts were coded for qualitative content analysis (Kuckartz 2014) using MAXQDA software with a mix of codes derived inductively and

deductively. As recommended by Kuckartz, significant deviations between encodings of identical interviews were extensively discussed until a consensual set of main categories could be agreed upon by all members of the research team. All interviews were then coded with this finalized code set. While the list of codes was extensive and covered a range of aspects of smart speaker use, in this chapter we focus on fatalism. The use of Pettenkofer's fatalism concept was inspired by research in a previous project (cf. Englert et al. 2019). Initially, all identified instances of fatalism were grouped in one code. However, after discussing the coded material, fatalism appeared to be more heterogeneous than anticipated. Furthermore, examples of it could be found not just in the fatalism category itself but also in other categories focusing on observation and surveillance. These codes were then subjected to a re-coding and re-analysis based on inductive findings from the material as well as an application of theoretical concepts from the literature referenced above. As a result, four subcodes of fatalism were derived: resignation (cf. Lutz et al. 2020), cynicism (cf. Draper and Turow 2019), trust, and pragmatic fatalism (cf. Pettenkofer 2017). These types are detailed in the following.

4. Four Shades of Fatalism

We propose that differentiating these aspects of fatalism offers a way to expand upon the debate outlined above on user reactions and strategies concerning corporate data practices. These different aspects emerged in several interviews and sometimes even in combination. The following four distinctions or shades of fatalism are therefore not to be understood as a typology of our interviewees, but as a disambiguation of the standpoints that users adopt to situate themselves vis-à-vis corporate actors and data practices, as well as to public debate on the issue. At the same time, these aspects also reflect how users evaluate what these data practices mean to them on a more general level.

4.1 Resignation

Resignation, as outlined above, is an attitude inherent to many users' data practices regarding IPAs and is fostered by online corporations (Draper and Turow 2019). It represents a form of individual surrender to an entity that is perceived as more powerful than oneself and impossible to influence. According to Pettenkofer, such resignation is what enables users to continue using

IPAs despite data concerns, since it is based upon the conclusion that surveillance via IPAs is negligible in comparison to all the users' data that has been collected already. Hence, this resignation does not render users apathetic but rather enables them to continue using IPAs and other surveillance-affording devices and services (Pettenkofer 2017). Our interviewees, however, discussed and justified their resignation in more differentiated ways and distinguished between different entities to whom they surrendered. For them, surrendering meant accepting that they were unable to influence the processing and capturing of their data by the IPAs and the companies behind them. What varied, however, were the entities or actors that interviewees identified as being the ones to whom they were obliged to surrender in order to continuing using IPAs. Furthermore, users described different ways of resigning to such entities. Some spoke about individualistic experiences, while many others talked about general notions and tendencies in society at large; some speculated on companies' rationales. Significantly, the consequences of resignation were not evaluated on an individual, but on a collective level.

"Well, I think that, for us, so to speak, the train has already left the station." (Beate W., l. 583–584)³

Entities to whom users saw themselves surrendering were often somewhat abstract. Above all, it was corporations that were accused of exchanging data on such a scale that consumers became transparent. Protecting one's privacy was seen as impossible in the face of surveillance perceived to be omnipresent in online and offline spaces.

"I think that we are transparent as customers or as consumers anyway and that [using a smart speaker] does not make any difference anymore." (Robin L., intv. 1, l. 551–554)⁴

As proof that companies were exchanging data without any possibility for users to intervene, interviewees cited personalized ads. Participants concluded that certain apps or devices and the companies behind them already had the kinds

3 German original: "Also der Zug ist schon abgefahren für uns, sage ich mal."

4 German: "ich dachte mir dann ja, also gefühlt ist man eh schon äh der gläserne Kunde oder der gläserne Konsument und [die Nutzung eines Smart Speakers] macht dann irgendwie auch keinen Unterschied mehr [...]."

of data that could be obtained by an IPA, making surveillance by the IPA negligible.

“We live in times of Facebook, don't we? That is, we look for something on Amazon and three seconds later, there is an ad on Facebook that fits what we were looking for just a moment ago.” (Jan-Ole S., intv. 1, l. 323–327)⁵

Resignation to a lack of data security inherent to IPA usage is therefore entangled with privacy concerns pertaining to other aspects of everyday life. Data capturing is perceived not only as inevitable but as something that has already taken place, as the reference to the “times of Facebook” and thus to the Cambridge Analytica scandal implies. Since the platforms already have the users' data, there is no point in worrying about the consequences of the IPA's data capturing. Resignation is therefore grounded in the assumption that it is already too late for everyone and not just for the individual.

“We can not get out of this.” (Beate W., intv. 1, l. 654)⁶

4.2 Cynicism

Cynicism, like resignation, addresses an entity, and therefore creates a relation between individuals, groups, and their environment. Cynicism differs from resignation, however, in that it expresses an antagonistic relationship towards a counterpart. The antagonism conveyed by our interviewees was most frequently expressed in claims that corporations were untrustworthy regarding data protection. This goes beyond resignation to corporations or state agencies portrayed as powerful and surveillance as inevitable. In addition, a cynical perspective distrusts these powerful actors (Lutz et al. 2020). As the following section shows, trust – and instances in which it is broken – played an important role in shaping interviewees' attitudes. As in research by Hoffmann and colleagues (2020), tech companies were perceived as powerful and uncontrollable, which led to feelings of powerlessness and of being at the mercy of plat-

5 German: “[...] wir leben in der Zeit von Facebook, ne? Ich meine, wir suchen bei Amazon suchen wir etwas und haben drei Sekunden später bei Facebook eine Werbebenachrichtigung von dem, was wir gerade gesucht haben.”

6 German: “Wir kommen aus der Nummer nicht raus.”

forms. In addition, users assumed that the actors concerned had bad intentions, such as evading taxation or EU law.

“What should Amazon be afraid of? It’s a multinational corporation, almost THE multinational corporation. And if you look at their revenue in the last few years and if you look at the effort of governments to get Amazon to pay taxes, in some areas, like in Europe, why should this topic be a red line that Amazon does not cross, that is somehow more relevant than other guidelines?” (Alex K., interv. 1, l. 510–518)⁷

In accordance with this perspective, software features that allow users to delete data, such as audio recordings of voice commands, were often dismissed as fake concessions towards users; an accusation supported by statements indicating partial or vague knowledge about IPA infrastructure. User settings on the Amazon and Google platforms enable audio recordings of IPA use to be deleted (cf. Pins et al, this volume). But our interviewees disregarded this, because they assumed that Amazon and other companies would have secret back-ups anyway in order to continue analyzing the valuable data.

“Well, I think that, if they want my private data, they are able to access the stuff that I deleted, too.” (Andrea S., intw. 1, l. 2870–2872)⁸

Privacy cynicism, like every fatalistic reflection pattern, makes it pointless to reflect upon certain topics, since the antagonist is too powerful to deal with. Government regulations and guidelines put in place by the companies themselves are seen as strategies to project an appearance of law-abidance. Trust towards the companies has already been so eroded that data control features are perceived as just another ploy to advance data collection. Tellingly, one in-

7 German: “Was hätten sie denn zu befürchten? Also es ist ja letztendlich ein multinationaler Konzern und äh fast schon DER multinationale Konzern. Äh wenn man sich anguckt, was die in den letzten Jahren an Umsätzen geschoben haben und äh was für einen Aufwand Staaten betreiben müssen, damit die über/ also damit Amazon überhaupt äh Steuern zahlt in manchen Regionen, beispielsweise in Europa, (.) warum sollte das ein Aspekt sein, der da irgendwo ausschlaggebend ist und wo dann die rote Linie ist?”

8 German: “Ja, also ich denke, wenn man/ wenn die, sage ich mal, meine privaten Daten haben wollen, dann äh können sie auch auf gelöschte Sachen zugreifen.”

interviewee described himself as “cynical” while putting forth his argument in the logic of privacy cynicism:

“Well, putting it like this involves some cynicism. However, in the end, I think this is correct. Isn't it? If I am really interested in a dataset, I will analyze it before I offer users the chance to delete that data so that they don't worry too much. Well, I put this more cynically than I intended (laughter).” (Alex K., intv. 2, l. 1397–1405)⁹

4.3 Trust

To identify trust as a mode of fatalism might seem counter-intuitive at first glance. When looking at fatalistic reflection patterns, however, it becomes clear that cognitive processes involving the idea of trust can be described as fatalistic: Trust enables actors to externalize responsibility by entrusting another actor (e.g., a company, experts, or governmental oversight more generally) to take care of their concerns and problems. Draper and Turow (2019) indicate in their discussion of privacy-related corporate communication strategies that tech companies obfuscate their data handling at the same time as insisting on it being safe and responsible. This leaves users with little choice but to believe a company's messages and trust it, or to distrust and refuse to engage with the company altogether. However, this conclusion was not supported by our interviewees' statements. Instead of trusting what companies claimed in their contracts or promised in advertisements, our interlocutors' views were based upon their own experiences and theories. These were probably also influenced by narratives, ads, etc. from the companies in question, but such material was not directly referred to or reiterated.

Of our interviewees whose statements reflected this fatalistic pattern, most expressed trust in Apple.

9 German: “Ja, im Endeffekt, da schwingt immer auch so ein bisschen Zynismus mit bei solchen Formulierungen finde ich. Aber im Endeffekt ist es halt auch genau das. Ne? Wenn man damit was anfangen möchte, mit so einem Datensatz, dann ist das normalerweise schon geschehen, bevor ich den Leuten die Möglichkeit gebe, den doch zu löschen fürs gute Gewissen. Also das war jetzt aber wieder zynischer formuliert (lachend) als ursprünglich gedacht.”

“That is, using Siri and only Siri and that’s it. Simply put, it’s convenient, it’s safe and there’s the data protection issue, too, of course.” (Julian R., intv. 1, l. 200–202)¹⁰

Julian Rieker justified his trust in Apple by comparing its corporate data practices to those of Amazon. He perceived the personalized ads that Amazon generates as something bothersome and annoying. In his view, Alexa is the unsafe IPA that hands over data to further companies and is non-transparent about what it captures and how it will be processed. Targeted ads were cited by Julian as well as by other interviewees as proof that surveillance was taking place.

“Apple doesn’t want to sell you the next pair of socks or razor blades. And with that lady in the Amazon speaker, I am not sure what [data] gets processed in the background. And if you happen to talk about Pampers, for whatever reason— then you’ll suddenly get shown ads for diapers. I haven’t even got a child! So, like (laughs), where’s this coming from? And that’s the thing. So, no, I don’t prefer the lady with A [Alexa, Amazon’s voice assistant].” (Julian R., intv. 1, 169–178)¹¹

This stance towards Amazon is further justified by Julian’s belief that Alexa constantly transmits data, whereas Apple’s IPA processes data locally.

“Well, Amazon processes everything in the Cloud. So everything you say is routed via an Amazon server and that’s not how it is with Apple, for example. Apple processes everything on the device itself.” (Julian R., intv. 1, l. 213–216)¹²

10 German: “Das heißt, mit Siri und ausschließlich mit Siri und/ und das war es. Einfach Komfort, Sicherheit eben auch, das Thema Datenschutz natürlich.”

11 German: “Apple will dir nicht unbedingt äh die nächsten Socken oder die Rasierkliegen verkaufen. Und bei der Amazondame im Lautsprecher, da bin ich mir nicht so ganz sicher, was da alles verarbeitet wird. Wenn du dich mal über Pampers unterhältst, warum auch immer, ne? Und auf einmal kriegst Werbung von Pampers angezeigt. So, ich habe gar kein Kind. Weißt (lachend) du so, wo kommt das auf einmal her? Und das sind halt so Sachen, ähm ja. Die Frau mit A ist nicht so der Favorit.”

12 German: “Naja, bei Amazon wird alles direkt in der Cloud verarbeitet. Also das heißt, das geht wirklich alles, was du sprichst, geht immer auf die Amazon Server und das hast du bei Apple zum Beispiel nicht. Apple wird/ verarbeitet alles erst mal auf den Geräten selbst.”

Trust is expressed here by comparing a preferred product and its provider to one seen as less trustworthy. The evaluation is justified by the claim that local data processing and the (perceived) absence of targeted ads indicate Apple's trustworthiness.

Trust thus appears as a form of fatalism that is experienced by most interviewees as positive, unlike other forms of fatalism. This is not surprising since endowing trust upon a powerful other is not a matter of giving in to power, but of making an active choice. Trust can furthermore be seen as the opposite of cynicism as it expresses non-antagonistic engagement with a more powerful entity. This does not necessarily indicate enthusiasm, but does point to the nuanced spectrum of fatalistic perspectives.

4.4 Pragmatic fatalism

Unlike the examples analyzed above, in some instances, interviewees spoke about potentially problematic corporate data practices with less of a focus on collective aspects than on their individual perspective. Drawing on Andreas Pettenkofer's terminology (2017, 143, our translation), we refer to this as "pragmatic fatalism". The main characteristic of this line of reasoning is that users either (a) decide from the outset not to think about an issue, or (b) that their perspective is primarily influenced by their personal circumstances.

(a) Many statements in the interviews clearly indicated that most users stopped thinking early on about the potential consequences of the data analysis resulting from their smart speaker use, or decided quickly that they did not care about privacy. They mentioned several reasons for simply accepting the data practices involved. One reason was "laziness", as some users put it. Others, however, rejected the allegation of laziness by explaining that they had difficulty understanding (1) the privacy settings of the devices, (2) the technical processes of commercial data analysis, and (3) the open-source tools and alternatives to commercial platforms that might be available. Some saw themselves as simply unable to understand such aspects, while others argued that smart speakers are all about convenience and that it would be inconvenient to have to do research to understand the workings of the devices. This line of thinking is consistent with Pettenkofer's (2017) understanding of fatalism, whereby not thinking about something is what allows one to proceed.

(b) Another pragmatic reason cited for not thinking about the data-related consequences of using a smart speaker is that users are already enmeshed in corporate data practices. Interviewees explained that they had put aside their

concerns about data collection via voice assistants once they realized how much of their data was already being collected through their use of smartphones and other devices and services. More specific fears about acoustic surveillance were rendered insignificant by the realization that smartphones also have microphones that could be hacked and tapped by hardware manufacturers or criminals or misused by third parties. Samuel Matthäi – working as a teacher while completing a degree –, for example, had initially been wary about allowing a smart speaker into the kitchen of his shared apartment. However, he then reflected that he had already been using Siri on his smartphone for a while, even in his own room. He explained:

“I think that, after some time, at a certain point in time, I realized that I was using many, many devices already that were able to record audio, and that this thing was just another one (laughter).” (Samuel M., intv. 1, l. 202–209)¹³

Contrary to the resignation or cynicism detailed above, the focus of pragmatic fatalist views was less on one's position vis-à-vis a powerful and opaque corporate oligopoly, but on personal experiences of using devices and (not) perceiving data-related consequences. Such experiences did not have to be made directly; learning how other users dealt with issues was also influential. Samuel Matthäi had initially felt uneasy when he saw his new girlfriend's children using an Amazon smart speaker. Over time, he came to see how practical and entertaining the device was for the children. In our second interview with Samuel, a few months after he and his roommates had installed a Google Nest device in their communal kitchen, he had bought an Alexa device for his own room as well. This trajectory points to the relevance of social context: devices are more likely to be accepted and adopted by people who encounter them in others' homes as part of everyday life, and they are less likely to be viewed critically by people who have had opportunities to engage with them themselves.

Here, another element comes to the fore: the motif of harmlessness. Contrary to cynical and resigned views, a pragmatic fatalist perspective is justified

13 German: “Ich glaube, ab einem gewissen Punkt ist das auch nicht mehr unbedingt/ also, ne? [Da] kommt man zu dem/ oder kam ich zumindest zu dem Entschluss, dass ich sehr, sehr viele Geräte benutze, die aufnehmen können. Und dass das jetzt halt einfach nur ein weiteres ist.”

by describing the situation as safe. This emerged in our interviews in five ways. (1) Users claimed that the way they used their device was benign, because they only used it for simple commands and requests – e.g., asking for a weather forecast, the time, or telling the device to set a timer or to play a particular song. According to these users, even if the data involved were to be analyzed, it would yield only trivial information about their household. In other words, the data concerned was declared harmless. (2) Others emphasized the harmlessness of the device itself. Many users cited the frequent occasions when a device did not understand a request as evidence that the AI in the background was not particularly perceptive and hence would not be able to analyze much of what was going on in their homes. Moreover, devices were also seen as harmless (3) because users could not imagine worse consequences of using them than being exposed to personalized ads. A further aspect of device harmlessness (4) was asserted by users who argued that their device brought a certain degree of comfort but emphasized that they were by no means reliant on smart speakers in the way they depended, for example, on their smartphone or laptop. In this way, smart speakers were portrayed as a ‘toy’ or something trivial and non-essential. Finally (5), users portrayed themselves as harmless. As Patrick Gensing – who uses the Apple HomePod system in his family home – put it:

“I know it’s an overused phrase, but who could possibly be interested in my conversations with my kids at home? It’s just not interesting to anybody. I consider myself to be boring, so I wouldn’t care if someone was listening to me.” (Patrick G., intv. 1, l. 375–381)¹⁴

In view of such harmlessness, thinking too much about the potential use of data collected and speculating on dangerous consequences thereof was dismissed by some as “paranoia” (Julian R.) or as an example of susceptibility to a “conspiracy theory” (Robin L.); i.e., as unnecessary, problematic, or pathological behavior. Such a view was substantiated by the fact that none of those interviewed mentioned any direct and negative consequences of smart speaker use, except for a few unexpected reactions and malfunctions (cf. Lutz and Newlands, this volume). This supports our proposal that in order to maintain their

14 German: “Ich weiß, es ist ein abgedroschener Satz, aber was interessiert denn irgendjemanden, was ich Zuhause mit meinen Kindern bespreche? Das interessiert vermutlich keinen Menschen. Also ich halte mich da für langweilig, (lachend), insofern wäre mir das auch egal, wenn da jemand zuhört.”

conviction that the device and its use are harmless, users have to actively refrain from delving into data protection discourse. This relates to the “positive thinking” mentioned by Pettenkofer (2017): When users see other users using the device effortlessly and thoughtlessly and without negative consequences, they assume that they too will be able to use the device without incurring harm.

5. Discussion

5.1 Fatalism

While this chapter is specifically concerned with smart speakers, users evaluate their use and problems within the wider contexts that shape their lives. One such context is the digital lifeworld of interconnected services that are, to a certain extent, always based on the analysis of user data. Another context is the user’s household, which is particularly relevant when devices are purchased for and used by all its members, who may have differing capabilities, needs, or interests.

When it comes to the cynical, apathetic, and resigned attitudes that other studies have identified among smart speaker users, we can confirm that our interviewees also viewed IPAs’ interfaces and corporate infrastructure as opaque and potentially problematic. At the same time, most did not express feeling bothered or frustrated by this but were inclined to disregard such issues – not just in their everyday use of the devices, but also when explicitly asked about their opinions in our interviews. Some completely refused to think about potentially problematic issues while others acknowledged in principle that there might be problems with corporate data practices. Both groups determinedly refused to make such issues *their* personal problem.

There is certainly a pragmatic aspect to such cynicism and resignation: it enables users to justify using the products and services despite acknowledging problematic aspects. This has been mentioned by Lutz and his colleagues (2020) as well as by Draper and Turow (2019). The users quoted in those papers and the terminology chosen in both suggest problematization by users that was, however, less prevalent in the interviews in our study. While we do not make any quantitative claims, we nonetheless suggest that there is not only hand wringing and negative views among users (cf., e.g., Hoffmann et al. 2016), but also a certain disregard of the topic of data privacy altogether, or it was raised as part of a more personalized evaluation. Users in our study who

said that they never thought about corporate data practices and surveillance were by no means unaware of the critical discourse about them in media and the public sphere. However, they actively chose not to personally investigate the claims and issues or relate them to their own personal situation and use of the devices.

Other users reported that they were less concerned with the overall discourse than with their own situation. In their view, just about everyone in society is already part of corporate online platforms. This was not seen as representing a gross power inequality with corporations tracking and exploiting users who have no choice but to make use of online services; instead, it was presented as a justification for deciding to use smart speakers while not denying privacy concerns. This is what we glean, for example, from Samuel's narrative detailed above. He explained how he overcame his initial skepticism towards smart speakers simply by being exposed to them following his failure to convince his partner that they were not suitable for children. His girlfriend showed him what fun her children had with the device. Moreover, Samuel's recognition that he had already been using a portable version of a smart speaker did not lead him to consider ceasing to use Siri on his phone, but to reconsider his skepticism and ultimately to decide to increase his use of voice interface technology.

Smart speakers are an interesting technology in relation to fatalism, especially as users often portray them as an unnecessary luxury, as something futuristic they wanted to try out, or as a toy. This is quite different from when high-school students talk about how essential it is to use social media in order to not be left out (cf. boyd 2014, Englert et al. 2019). Such peer pressure does not tend to be experienced in relation to smart speakers, which have not been as widely adopted as smartphones. In 2020 in Germany, using a smart speaker was perceived as more of a personal choice than using a smartphone, which had come to be seen as essential in order to participate in much of everyday life. As such, the resigned and cynical arguments of users cannot really be explained by inevitability, since choosing not to use a smart speaker would not necessarily bring a great reduction in comfort or social standing. This argument does not hold for certain users, such as those with physical or visual impairments, who would stand to lose a great deal more by rejecting smart speakers.

5.2 Domestication

A progression from skepticism to adoption points not only to the affective dimension of technology use (cf. Bösel and Wiemer 2020), but also to a process that has been extensively explored in the field of “domestication” research (e.g., Bakardijeva 2005). Silverstone, Hirsch, and Morley (1992, 18) argue that media are not just consumed as content but also as object – collectively, in a household. The authors assert that this process already begins even before the media object enters the home. These arguments can be convincingly applied to smart speakers as well. Silverstone and colleagues note how media are “appropriated” (1992, 16) and adapted to fit in with domestic routines and lifestyles. Metaphorically speaking, media come into the home as something “wild” that needs to be “tamed” (Waldecker and Hector 2023). But just as the process of domestication turned hunters into shepherds and foragers into farmers, the domestication of media also has the potential to change the domestic “moral economy” (Silverstone et al. 1992) by inciting the establishment of new evaluations and everyday practices.

However, this is not simply a matter of a slow habituation to new devices and services. As becomes evident in the way Samuel’s views changed, elaborated above, the “taming” process is social: it is shaped by discussions with peers and household members. In her study on the private adoption of the internet in the early 21st century, Maria Bakardijeva highlights how new users were guided by “warm experts” (2005, 99), i.e., individuals within reach who were more knowledgeable than the users who asked for their help. Bakardijeva notes that these warm experts not only provided the skills necessary to get private internet access up and running, but also motivated users to actually try using online services. Nowadays, some of this motivation and enthusiasm for smart home devices is promoted by social media tech influencers, which Stephen Neville, accordingly, terms “online warm experts” (2021). While the input from these actors is no doubt relevant, our interviewees reported that their personal contact with other people who used smart speakers was even more significant in arousing their interest in trying out a smart speaker themselves. As such, “appropriation” (Silverstone et al. 1992) is not just an individual task and is not just about the device itself, but involves finding a personalized stance to appropriate the mediatized discourse on online privacy and surveillance. As our study and others mentioned above have shown, users are well aware of the critique of the data-based online economy and the potential for surveillance. How they relate their own personal, domestic, specific media use

to this discourse is, to a certain extent, also influenced by their interaction with other users. It also indicates that this “appropriation” is never complete but is a practical task, an ongoing activity that changes over time (Silverstone et al. 1992, 19).

In sum, the domestication perspective can also be used to paint an empirically rich picture of how users experience data practices and how they do and do not deal with them in everyday life. It can also help us understand how positive, negative, and disinterested views on the issue are formed and how they in turn relate to everyday practice.

6. Conclusion

While the data from our interviews, complemented by results from the media-linguistic strand of our research project (cf. Habscheid, Hector, and Hrnčal, this volume), can only provide partial insights into the wider embedding and enmeshing of data practices in everyday life, they have nonetheless allowed us to showcase how the fourth shade of fatalism, the most openly pragmatic kind, is connected to day-to-day experiences of using IPAs and the circumstances that shape them.

As Pettenkofer (2023, 65) argues in his most recent publication on fatalism, fatalism creates “a new routine of selectively avoiding reflection, which creates new, self-sustaining forms of selective attention”. Support for this assertion is found in users’ emphatic insistence on the harmlessness of using IPAs. With this focus on harmlessness, they steer the discourse away from the potential dangers of corporate data practices and the surveillance inherent to IPAs. Users’ “civil inattention” (Goffman 1972, 385) to these topics makes sense: interviewees mentioned that they were unable to assess the actual data practices that take place in the back-end, which are controlled and obfuscated by companies (Draper and Turow 2019). Hence, they can never know whether or how these data practices might affect them. As most of them had not personally encountered any negative consequences directly traceable to the data recorded through their IPA use, they had no reason to concern themselves with what they could not know anyway – thus, their pragmatic negligence of the data protection issue. Therefore, it is not without justification that many users see their smart speaker use as “mostly harmless” (Adams 1979) having not personally experienced noticeable harm. We would agree – at the level of the individual –

but less so when taking into account the analytical potential of the data collected from thousands of households.

Further research is needed to elucidate how fatalistic practices and attitudes are connected to specific circumstances (Pettenkofer 2023). The debate on privacy in media studies and connected fields, as traced above, has moved away from an individualistic focus to a more holistic picture, urging the need to consider corporate responsibility and the ways infrastructures and platforms present users' choices. To a certain extent, this debate mirrors the discussion on the individual and collective responsibility for climate change¹⁵. In Germany, climate change is now generally acknowledged to be a growing concern. Some voices in the discourse claim that consumers' choices can make a substantial contribution to increasing or reducing greenhouse gas emissions. This individualized allocation of responsibility has been countered, in recent years, by perspectives that emphasize the culpability of corporations (e.g., by showing how oil and gas corporations helped create narratives that focused on the "carbon footprint" of individuals in the first place, cf. Mann 2021). Regardless of these debates, individuals are, given the circumstances, often unable to avoid actions that produce carbon emissions even when they know about the negative effects. Certain infrastructural arrangements make it necessary for individuals to take a car to work or to work in carbon-intensive industries – or, on a more general level, such circumstances make it necessary for people to work in jobs that they find boring, degrading, or unacceptable (Graeber 2018; Chibber 2022, 106). From this point of view, the fatalism of tech users vis-à-vis data protection is by no means exceptional, but just one instance of a phenomenon that is constitutive of modern societies (Pettenkofer 2023). As such, exploring the mutual dissonance between collective *Sein* (being) and individual *Bewusstsein* (consciousness), so to speak, could offer a productive approach for investigating how individuals deal with problematic situations that can only be changed for the better if individuals address them not individually, but collectively.

15 The particularities of dealing with crises such as climate change via digitalization is an important aspect of the follow-up project of the research project this chapter is based on.

References

- Adams, Douglas. 1979. *The Hitchhiker's Guide to the Galaxy*. London: Pan Books.
- Bakardjieva, Maria. 2005. *Internet Society: The Internet in Everyday Life*. London: Sage.
- Barnes, Susan B. 2006. "A Privacy Paradox: Social Networking in the United States." *First Monday*. <https://doi.org/10.5210/fm.v11i9.1394>.
- Bösel, Bernd, and Serjoscha Wiemer, eds. 2020. *Affective Transformations. Politics – Algorithms – Media*. Lüneburg: meson press.
- boyd, danah. 2014. *It's Complicated. The Social Lives of Networked Teens*. New Haven, CT: Yale University Press.
- Chibber, Vivek. 2022. *The Class Matrix. Social Theory after the Cultural Turn*. Cambridge, MA: Harvard University Press.
- Draper, Nora A, and Joseph Turow. 2019. "The Corporate Cultivation of Digital Resignation." *New Media & Society* 21 (8): 1824–39. <https://doi.org/10.1177/1461444819833331>.
- Englert, Kathrin, David Waldecker, and Oliver Schmidtke. 2019. "Un/Erbetene Beobachtung. Bewertungen richtigen Medienhandelns in Zeiten seiner Hyperbeobachtbarkeit." *Digitale Bewertungspraktiken. Für eine Bewertungssoziologie des Digitalen*, edited by Jonathan Kropf and Stefan Laser, 215–36. Wiesbaden: Springer VS.
- Gandy, Oscar. 1989. "The Surveillance Society. Information Technology and Bureaucratic Social Control." *Journal of Communication* 39 (3): 61–76.
- Graeber, David. 2018. *Bullshit Jobs. A Theory*. New York: Simon & Schuster.
- Goffman, Erving. 1972. *Relations in Public*. New York: Penguin.
- Hargittai, Eszter, and Alice Marwick. 2016. "What Can I Really Do? Explaining the Privacy Paradox with Online Apathy." *International Journal of Communication* 10: 3737–57.
- Hector, Tim, David Waldecker, Niklas Strüver and Tanja Aal, eds. 2023. *Taming Digital Practices: On the Domestication of Data-Driven Technologies*. Digital Culture & Society 9 (1).
- Hoffmann, Christian P., Christoph Lutz, and Giulia Ranzini. 2016. "Privacy Cynicism: A New Approach to the Privacy Paradox." *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* 10 (4). <https://doi.org/10.5817/CP2016-4-7>.
- Khan, Shamus, and Colin Jerolmack. 2013. "Saying Meritocracy and Doing Privilege." *The Sociological Quarterly* 54 (1): 9–19.

- Kuckartz, Udo. 2014. *Qualitative Text Analysis: A Guide to Methods, Practice & Using Software*. Los Angeles: Sage.
- Lauer, Josh. 2010. "The Good Consumer. Credit Reporting and the Invention of Financial Identity in the United States, 1840–1940". *Enterprise and Society* 11 (4):686–94.
- Lengwiler, Martin. 2004. *Privacy, Justice and Equality: The History of Privacy Legislation and Its Significance for Civil Society*. Discussion Papers 2004–503. Berlin: Wissenschaftszentrum Berlin für Sozialforschung.
- Lovink, Geert. 2019. *Sad by Design. On Platform Nihilism*. London: Pluto Press.
- Lutz, Christoph, Christian P. Hoffmann, and Giulia Ranzini. 2020. "Data capitalism and the user: An exploration of privacy cynicism in Germany". *New Media & Society*, 22(7): 1168–187. <https://doi.org/10.1177/1461444820912544>.
- Mann, Michael E. 2021. *The New Climate War. The Fight to Take Back Our Planet*. New York: PublicAffairs.
- Neville, Stephen J. 2021. "The Domestication of Privacy-Invasive Technology on YouTube: Unboxing the Amazon Echo with the Online Warm Expert." *Convergence* 27 (5): 1288–307. <https://doi.org/10.1177/1354856520970729>.
- Norberg, Patricia A., Daniel R. Horne, and David A. Horne. 2007. "The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors." *Journal of Consumer Affairs* 41 (1): 100–26. <https://doi.org/10.1111/j.1745-6606.2006.00070.x>.
- O'Reilly, Tim. 2012. "What Is Web 2.0: Design Patterns and Business Models for the Next Generation of Software". *The Social Media Reader*, edited by Michael Mandiberg, 32–52. New York: New York University Press. <https://doi.org/10.18574/nyu/9780814763025.003.0008>.
- Pettenkofer, Andreas. 2017. "Fatalismus. Über eine vernachlässigte Stütze sozialer Ordnung." *Berliner Journal für Soziologie* 27 (1): 123–50. <https://doi.org/10.1007/s11609-017-0339-1>.
- Pettenkofer, Andreas. 2023. "Three Types of Fatalistic Practice." In "Weltbeziehung" – *The Study of our Relationship to the World*, edited by Hartmut Rosa, Jörg Rüpke, and Bettina Hollstein, 63–99. <https://www.campus.de/e-books/wissenschaft/soziologie/weltbeziehung-17937.html>.
- Silverstone, Roger, Eric Hirsch, and David Morley. 1992. "Information and Communication Technologies and the Moral Economy of the Household." In *Consuming Technologies: Media and Information in Domestic Spaces*, edited by Roger Silverstone and Eric Hirsch, 13–28. London: Routledge.
- Taddicken, Monika, and Jan-Hinrik Schmidt. 2016. Entwicklung und Verbreitung sozialer Medien. In: *Handbuch Soziale Medien*, edited by Jan-Hinrik

- Schmidt and Monika Taddicken. Wiesbaden: Springer VS. https://doi.org/10.1007/978-3-658-03895-3_1-2.
- Turow, Joseph. 2021. *The Voice Catchers: How Marketers Listen in to Exploit Your Feelings, Your Privacy and Your Wallet*. New Haven, CT: Yale University Press.
- Waldecker, David and Tim Hector. 2023. "A Praxeological Approach Towards the Domestication of Connected Media Technologies." *Digital Culture & Society* 9 (1): 5–22. <https://doi.org/10.14361/dcs-2023-0102>.
- Witzel, Andreas, and Herwig Reiter. 2012. *The Problem-Centered Interview. Principles and Practice*. Los Angeles: Sage.
- Zuboff, Shoshana. 2020. "You Are Now Remotely Controlled." *The New York Times*, January 24, 2020, sec. Opinion. <https://www.nytimes.com/2020/01/24/opinion/sunday/surveillance-capitalism.html>.
- Zuboff, Shoshana. 2019. *The Age of Surveillance Capitalism*. London: Profile.

