MedieKultur | Journal of media and communication research | ISSN 1901-9726

Article – Theme section

Trust, Disconnection, Minimizing risk and Apathy

A Compass of Coping Tactics in Datafied Everyday Lives

Jannie Møller Hartley and Sander Andreas Schwartz

MedieKultur 2020, 69, 11-28

Published by SMID | Society of Media researchers In Denmark | www.smid.dk

The online version of this text can be found open access at www.mediekultur.dk

Abstract

This paper investigates how audiences are coping with digital platforms in their everyday lives. Empirically grounded in focus groups carried out in Denmark with a total of 34 participants of different ages and educational backgrounds, we present the results of an analysis of audiences' coping tactics in relation to tracking data, collecting data and mining data. Based on the analysis, we find four overall tactics: coping by absence, coping by trust, coping by minimizing risk and coping by apathy. We argue that these different coping tactics are employed differently depending on the context of the digital routines, the data collected (sensitive vs. non-sensitive data), and the dependence of the platform (private vs. public, national vs. international platforms and apps). These contextual factors are presented in an analytical model—a coping compass—for studying individual users' coping tactics in their datafied everyday lives.

Keywords

Datafication, everyday life, coping, trust, data anxieties, focus groups

Introduction

In most of the world, internet connectivity and associated digital literacies are increasingly necessary in the activities and functions of everyday life. Practices such as searching for information, communicating with friends, shopping, and many more activities and routines of everyday life are extensively mediated through digital platforms based on data processing codes and algorithms.

The increasing reliance on digital services produces vast amounts of behavioural data that service providers exploit in order to maximize profit. The phenomenon that enables this commercial exploitation of user data has been referred to as datafication, defined as "the transformation of social action into online quantified data, thus allowing for real-time tracking and predictive analysis" (Mayer-Schönberger & Cukier, 2013, p. 198). Some researchers argue that datafication is based on a misguided ideology (van Dijck, 2014), while others believe that the datafication of user data is an intrusive and manipulative threat to democracy (Zuboff, 2019). An increasing number of studies are exploring datafication in many domains of everyday life, including health (Ruckenstein & Schüll, 2017), governance and policing (Dencik et al., 2018; Smith & O'Malley, 2017), everyday spatiality (Sumartojo et al., 2016) and sport (Millington & Millington, 2015). The research on datafication has provided us with important knowledge about how different populations and domains are using data and the possible consequences thereof. However, with this study, we wish to direct attention to the potential agency of the users of digital platforms.

In the context of this study, we approach datafication as the rendering of everyday practices into data and we ask how people act upon the experiences they have in their encounters with data in everyday life. Thus, by means of a bottom-up approach, this article seeks to direct scholarly attention towards ordinary users' self-reflexive perception and discursive articulation of their everyday datafied practices. We operationalize these articulations analytically as coping tactics, inspired by de Certeau's (1988) definition of tactics as practices of resistance and appropriation by the seemingly less powerful in response to asymmetric structures of power.

Previous research has identified a privacy calculus for assessing the pros and cons of media use, while also noting a privacy paradox (Hargittai & Marwick, 2016; Young & Quan-Haase, 2013) based on a misalignment between users' discursive concern for privacy issues related to datafication and their everyday practice on social media platforms. This article contributes to the body of literature by including public service platforms, private digital services and apps in the empirical scope. Following the expansion in scope, we present a coping tactics compass, which provides further evidence and nuanced understanding of the factors involved in the weighing of the the pros and cons as they are experienced by the users themselves.

Focusing on coping tactics as forms of resistance directs us towards the smaller acts which happen in the flow of the everyday but nevertheless constitute agency on the part of the users (Picone et al., 2019). The views from the users are presented in the analytical

part of this article, presenting four types of coping and appropriation tactics found across the material. Before presenting the four coping tactics as an analytical framework, we briefly situate our research in relation to existing literature.

The literature on everyday experiences of datafication

As Kennedy (2018, p. 18) argues, little attention has been paid to "ordinary, non-expert folks' thoughts and feelings about how their data are used, shared, and acted upon", which, according to Kennedy, "is as true in data practice and data policymaking as it is in academic research into the growth of big and small data". Kennedy points out that although there have been a few surveys on public attitudes, these surveys focus overwhelmingly on single issues such as privacy and surveillance: she calls for a "much more qualitative understanding of how different people experience, negotiate, trust, distrust, or resist big data and data mining" (Kennedy, 2018, p. 18).

Initial attempts have been made. For instance, Kennedy herself, together with colleagues in Norway and Spain, has examined users' attitudes towards data mining through scenarios in focus groups, concluding that almost all participants responded negatively to the fact that Facebook ignores users' privacy settings when giving information to third parties, but evaluations of scenarios differed otherwise. For many respondents, attitudes seemed to be influenced by factors related to the fairness of data mining practices, such as the sensitivity of the information, the purpose for which the information is used, and whether or not the user is aware of the monitoring (Kennedy et al., 2017, p. 280).

Bolin and Andersson Schwarz's (2015) study of media companies' user interpretation and institutional translation of big data (so-called "heuristics of the algorithm") includes an examination of media users' perception of their changing roles in the present information society (Bolin and Andersson Schwarz, 2015, p. 10). Through focus groups and individual interviews with Swedish media users about "online media use, questions of privacy, digital tracking, the benefits and downsides of SNS use, etc.", Bolin and Andersson Schwarz (2015) show how "a dialectic of the digital" presents itself "as an opportunity structure (or informational possibility), and as a burden (or restraint)" (p. 6). The focus of their study was again on social media sites, but it captured the complexities involved in users' negotiation of this dialectic.

Elsewhere, this observation has been described as "information asymmetry" (Brunton & Nissenbaum, 2015, p. 3, quoted in Pangrazio & Selwyn, 2018, p. 420), where the data about us are collected in circumstances we may not understand, for purposes we may not understand, and are used in ways we may not understand, and it has initiated appeals for developing user-citizens' data literacy (e.g. Gray et al., 2018; Pangrazio & Selwyn, 2018). Andrejevic (2014), who similarly conceptualizes this asymmetry as a "big data divide", has demonstrated how the lack of knowledge "about possible uses of personal information and the absence of any discernible negative impact of these uses" (p. 1682), alongside

a lack of options, leaves people with an "expressed sense of powerlessness vis-à-vis the arrangements that structure the collection and use of personal information" (ibid.). Based on a national telephone survey in Australia and individual and focus group interviews, Andrejevic reached the conclusion that "despite the persistent focus on privacy issues in both academic research and popular press coverage, privacy arguably takes a backseat to an underlying sense of powerlessness" (ibid.). Similarly, "digital resignation" has been suggested by Draper and Turow (2019) as a rational response to consumer surveillance. They further argue that routine corporate practices encourage this sense of helplessness (Draper & Turow, 2019). However, in this paper, we want to focus specifically on the agency of users in situations which might be considered difficult and troublesome for users, but to a varying degree are conceptualized as tactics.

In the literature, special interest has been shown in what has been labelled the 'privacy paradox' (see Gerber et al., 2018, for a literature review), which refers to studies that show how privacy of personal data is an important issue, and yet users rarely make an active effort to protect their data and often even give it away voluntarily (Gerber et al., 2018, p. 226). This is, of course, accompanied by a wide range of critical claims that users' control over the processing of their data appears mostly lost (Bottis & Bouchagiar, 2018), that existing privacy regimes inadequately address current big data challenges (Crawford & Schultz, 2014), and that the binary choice given by online privacy notices of either consenting or abandoning a desired service was not what privacy architects envisioned (Cate & Mayer-Schonberger, 2013).

Dencik and Cable (2017) examined attitudes among the public and among activists following the Snowden leak, arguing that the lack of transparency, knowledge and control over what happens to personal data online has led to feelings of widespread resignation, not consent, to the status quo that speaks to a condition they identify as "surveillance realism". They understand this to entail an unease among citizens about data collection alongside the simultaneous active normalization of surveillance that limits the possibility of enacting modes of citizenship and of imagining alternatives (Dencik & Cable, 2017). Insights such as these have led some researchers to focus on data anxieties, these being "the anxieties that are experienced, expressed and imagined both in the datafied present and as yet unknown datafied futures" (Pink et al., 2018, p. 3). According to Pink and her colleagues, trust is an associated concept in this context, since it is through trust, generated by everyday improvisatory actions, that these anxieties are eased. Thus, Pink et al. (2018, p. 3), departing from a design anthropological theory, define trust as "a feeling that specifically refers to the ability to be able to move on and do something in the immediate future. It need not involve absolute certainty, but entails feeling and knowing enough to be able to take the next step". Empirically, Pink and her colleagues undertook ethnographic fieldwork at sites in Barcelona and Melbourne, which host communities of individuals, companies and organizations with a focus on emerging technologies. The researchers focused on the element of "the anxieties associated with the kinds of every-

day data that people handle in the course of their mundane daily routines of home and work life" (Pink et al., 2018, p. 4), showing how their participants experienced and articulated such anxieties, as well as the measures, trade-offs and tricks people undertake to cope with them, and how people are subsequently able to trust that their data will be sufficiently safe. Thus, Pink et al. (2018) advance "a processual theory of trust that maps out how people cope with the inevitable uncertainty and contingency of the emergent circumstances of everyday life" (p. 12).

From these studies, we can draw firstly that people are feeling a sort of unease about their datafied practices; secondly, that the users are negotiating the pros and cons in this dialectic process; and thirdly, that knowledge or lack of knowledge plays a role.

While this vast body of literature and approaches to big data and trust certainly meet Kennedy's (2018) call for a more qualitative approach, much work is still needed to understand how people experience and negotiate their encounters with powerful actors' data collection, data analysis, searches, sorting and predicting in their everyday lives. The study by Pink et al. (2018) is focused on data storage and the participants were primarily tech-savvy and already interested in technology as a part of their job. However, we wish to contribute to lay people's (people of different ages and backgrounds) everyday dealing with data in the broader sense, not just data storage, but also data mining on the part of companies and platforms who collect and utilize data for commercial and non-commercial purposes. The focus on everyday tactics is useful in the context of this study; however, as we build our theoretical framework around de Certeau's (1988) notion of coping tactics, we are more concerned with what matters for how non-expert citizens experience and cope with data anxieties in their everyday lives.

Hence, in this study, we wish to examine these diverse practices in a broader context of digital platforms; we also aim to move beyond privacy and surveillance issues and questions of knowledge. In the next section, we elaborate on how we understand such tactics in datafied everyday life theoretically.

Theoretical framework: Everyday resistance tactics

The internet is a complex and networked infrastructure within which users must navigate and devise "ways of operating or doing" the everyday (de Certeau, 1988, p. 11). The online infrastructure is designed by powerful media institutions (such as Google and Facebook), who develop sophisticated strategies to control and manipulate users and the data they provide. However, the users of online services are not simply subjected to such strategies passively or without power. In his discussion of everyday life practices, de Certeau (1988) noted how tactics are commonly employed by people (in their capacity as consumers, readers, audiences and so forth) to shape or influence constrained environments (e.g. technical, economic or political systems) and practices. Tactics are described as practices of resistance and appropriation enacted against the strategies of larger and more power-

ful systems and actors. As de Certeau made clear, consumers and users are not passive—they work within the systems in which they find themselves, and appropriate and subvert their practices through various tactics of "making do" (de Certeau, 1988). According to Willson (2017) it is the intersection of institutions' strategies and users' tactics that lends shape to everyday life (Willson, 2017, p. 140).

An example of the increasingly complex development of control strategies is the algorithms used by many online services and social media platforms. Like Willson (2017), we understand algorithms to hold a potential to operate semi-autonomously by algorithmic delegation, a term developed from Latour's work (Latour & Johnson, 1998). Thus, the delegated execution of everyday practices is understood to be accomplished by default, without the need for interaction with, or knowledge of, human users or operators (Willson, 2017). Algorithmic delegation strives to work smoothly and unobtrusively, but this is not simply motivated by the service provider's ambition to make the user experience more convenient and gratifying. Algorithmic delegation can also be interpreted as a systemic attempt to strategically obscure the datafication and unrestrained colonization of the everyday lifeworld (Couldry & Mejias, 2018). Dencik and Cable (2017) use the term "chilling effects" (p. 764) to describe moments when users become aware of data surveillance and choose to moderate their own online behaviour. In this sense, a chilling effect may have a pacifying effect or create a sense of resignation in users. However, through the understanding of everyday online tactics, research can adopt a more active and nuanced understanding of users' response to institutional strategies. While we acknowledge the need to take a critical approach to powerful actors, we argue that it is just as important to acknowledge the agency of users beyond surveillance and privacy issues. This perspective is rather overlooked in the dominating critical theoretical approach to datafication, as surveillance and privacy studies tend to render the individual powerless in the face of a systemic power—i.e. "surveillance capitalism" (Zuboff, 2019). In this article, we question the view of the powerless, anxious user on the one hand and the autonomous invisible algorithms on the other by specifically focusing on the practices of the users as productive resistance and appropriation in their datafied everyday lives.

Methodology

This study is based on four focus groups of between four and nine participants conducted in Roskilde, Denmark, in autumn 2018 and spring 2019. The focus groups had a total of 34 participants, who were male and female citizens of Denmark divided into mixed groups according to age (ages 18–35 and ages 35–60) and education level (0–3 years of education/3 or more years of education beyond secondary school). The four groups were separated according to age and education in order to increase homogeneity and productivity in group discussions (Bloor et al., 2012) while allowing comparison across the groups.

The material is part of a larger project on the datafication of everyday lives carried out at Roskilde University.

The demographics of these groups are not statistically representative in any sense; rather, they collectively represent a cross-section of society. In this respect, the categories are not entirely mutually exclusive. As Barbour and Kitzinger (1999, p. 7) put it, focus groups "encompass diversity and compose a structure" that is guided by the research questions. However, we have deliberately organized the focus groups to allow us to consider the nuances of diversity with regard to understanding, attitudes and experiences (Kitzinger, 1994).

Denmark has a high adoption rate of the internet in general (97%) and Facebook in particular (73%). Furthermore, the Danish population has a high level of trust in established news institutions in general and public service channels in particular (Newman et al., 2018). Apart from the media institutions, Danish citizens also have high trust in government institutions in general, as well as high GDP and education levels based on a strong welfare state system (OECD, 2019).

Our focus groups were initiated with a broad discussion on everyday use and habits on a number of different digital platforms and services. Each time the participants mentioned a new digital service or platform that had not been brought up before, we asked them to note this down on a Post-it, which was put on a wall. In the next phase, we discussed the concept of trust in institutions and platforms by rating some of the platforms with regard to trust and usage. This was done in order to open up the discussion on how they were coping with mistrust and data anxieties. The last phase was more specifically about coping tactics. To encourage discussion, we provided screenshots of consent forms and cookie policies, as well as e-mails about GDPR from various institutions.

The focus groups where recorded, transcribed and read by all researchers involved in the project. After this, we discussed the emerging key coping strategies from the interviews together and related them to key theories and research questions. The participants are anonymized in the analysis.

In the remaining part of the article we present the results of the analysis. The first part presents the coping tactics in terms of resistance strategies towards the datafication of everyday life. The four overall coping tactics are: 1) coping by disconnection; 2) coping by minimizing risk; 3) coping by trust; and 4) coping by apathy. Following this, we discuss how these tactics are related to the contextual factors of evaluated dependence and evaluated risk of their datafied practices, and we present the analytical model of the coping compass to illustrate how the coping tactics relate differently to each of the contextual factors.

Coping by disconnection

First of all, we had a small group of people who were coping by disconnecting from digital platforms. They felt so worried about how they were profiled, surveyed, etc. that they

chose not to be on digital platforms if they could avoid it. The problem for these people was that many platforms could not be avoided—for example, those belonging to the Danish government regarding schools or health. The participants thus had to cope with this in a similar way to those participants who did not cope with data anxiety by disconnecting, instead engaging but being fully aware of the paradox that this entailed. The data material showed that being absent was often about maintaining control of one's digital presence, as this female participant describes:

> So, basically, I think that nobody really knows what happens with big data. I think there are many who would like to say that they know a whole lot, and I also think that there are a whole lot of stories that we can't really sort through either. And I don't like that. I don't feel comfortable when I don't know what the truth is and when I can't navigate. And just because you are a little smart person with a computer, you can fool me or something because I do not have the knowledge myself. I do not like that. So that's actually what makes me abstain from it. And it's not because I don't want to, because I really want to be modern and things like that. It is not at all. But uh, I just haven't ... it's out of my control (Older group, higher education, IP1).

She explains how she is not on Facebook, and is absent from social media in general, because she feels she cannot know what will happen to her data and feels a sort of asymmetry of power, where the platform providers are trying to con her. It was quite clear that she had a very low level of trust, and the many cases of data leaks she could refer to just confirmed her decision to be absent. However, this participant also emphasized several times how she did not feel she needed Facebook in her everyday life, apart from when her daughter recently had to join a club which demanded that her mother had a Facebook profile, as the daughter was too young.

A more minimal disconnection coping strategy was detoxing, or avoiding using a specific platform for a period. For example, one younger participant told how he removed the Facebook app every couple of months and would then install it again. This showed how the participants are navigating between, on the one hand, dependence on the platforms, as they are being used for school, work or other activities that the participants are a part of; and, on the other hand, the fear of their data being used for purposes beyond their control.

In a similar example, we see how the chilling effect is experienced twofold. Firstly, as above, these effects differ in various social circumstances. For example in relation to privacy in the immediate social network—for example, your partner not finding out what Christmas present you have bought for him or her; and secondly, in relation to fears of surveillance by the digital platforms, as this participant explains on her feeling of weirdness about the fact that Google Maps already knows where she is going when she gets in the car:

> I think it's weird because it's like it's persecuting me, and I don't think it's something I've said yes to, where the streaming services I've signed a concent form and subscribed, and Borger.dk I have also said yes, to online banking and so on. But this, so it is not something I remember saying yes to. And it is very cool to say that it now takes 1 hour and 14 minutes to work on a job today. And you just think 'how do you know I'm going to Nykøbing Falster today?' It's not every day I drive to Nykøbing Falster (Older group, higher Education, IP2).

Coping by disconnection was not only a chosen strategy in relation to social media platforms, but also in relation to specific sites that were not trusted, such as the Chinese shopping site Wish. This participant explains how she gets annoyed with them seemingly knowing what she needs before she knows it herself:

> It's like, 'oh yeah, isn't your need just to have this thing shaped like Batman?' No, it is f* not. It is too unethical in a way. And I'm pretty sure they probably have a giga database with a lot of information. I don't want to be part of it. So, I made the choice, that I do not have to (Older group, higher education, IP2).

When choosing not to act, much of the reflection on this form of engagement revolved around identity-driven issues rather than content-driven ones. By this, we mean that disconnection can be seen as a productive practice, in that it takes a conscious and substantial effort to refrain from being present on these platforms, which only seems possible when it comes to platforms where dependence is low—for example, shopping sites and social media platforms. On the other hand, when risk is perceived as high—for example, involving data about their health—the participants were inclined to trust that the organization or platform would keep their data safe and refrain from using the data for purposes to which the participants had not given permission or consent. Before we take a closer look at coping by trust, we will present how some data anxieties led the participants to engage in ways that could minimize the risk they felt that these platforms posed.

Coping by minimizing risks

The second strategy we found in the material was chosen as a consequence of being too dependent but nevertheless wanting to feel less worried. Coping by minimizing risk is thus characterized by the usage of various digital platforms but engaging in specific ways to avoid putting oneself 'at risk'. 'Risk' usually referred to other people obtaining data or content about them that they felt was private, or their data being used in ways that were not able to control. Such a tactic involved making themselves invisible—for example, the participants talked about how they would put a sticker on their camera, delete cookies or use secret browsing. When asked directly, though, the participants felt ambivalent about deleting cookies, as these were sometimes also an advantage for example remembering previous searches and so on. These coping acts were also about getting 'fair' treatment, as the participants felt that the algorithms would show them a price according to previ-

ous searches they had done. This participant explains why he is deleting cookies, but the quote also illustrates that he is in doubt whether it has any effect:

> Yes, I do [delete cookies] because I don't want them to have information about me all the time. But I don't know if they have the data anyway. So, you become like that ... I think that maybe I'm not here a little bit, I'm trying to be safe… (Younger group, higher education, IP6).

We see the ambivalence between being dependent on usage but trying to minimize the risk felt by using the platforms. Ambivalence was also seen in the ways these tactics were talked about: they at times described themselves as "someone with a tin foil-hat." For example, this participant explained why it is important to turn off the geolocation setting on her phone:

> But I would also say, without it sounding really silly, but I do not have my mobile turned on geo-tracking either. The fact that it can track where I am. I think that is totally creepy (Older group, higher education, IP1).

We see in the material that the participants are aware of the paradox of posting, because something seems private—for example, the Messenger app—and at the same time they know that it is never completely private. This participant, for example, explains how it would be too much if he had to go around worrying all the time, so he chooses just to have a critical approach:

> Now, all I post is private—after all, it is for the ones who are my alleged friends, the ones I think have an interest in seeing these things. But, of course, you change and try to give it a little more critical sense, but I can't manage to be scared all the time. I cannot (Older, higher education, IP3).

The minimizing risk coping tactic also involved things like saying no to things by default—for example, pop up boxes, non-posting—that is, mainly lurking on platforms but not posting anything yourself. This involved carefully selecting what information the platforms can and cannot have, but again we see in this quote that the risk is not so much related to what the data are being used for, but to protect themselves from identity theft, or to avoid someone being able to figure out that their house is empty:

> But I'm not putting stuff up about my holiday, for example, cause imagine who can then see that I'm on holiday and commits that famous burglary despite all the alarms we have, right? So, I have no confidence in Facebook. I'm pretty sure they sell all my information, so it's my job not to give them much. But it's okay that they know that I am a woman and when I have a birthday. I don't care… (Older, Higher education, IP4).

One participant explained having a second email for platforms or apps that she wants to use but where she wants to avoid her email being used by the platform to send out advertising, etc:

> So, I would say that I actually created a specific email for those things, which is one only for some shitty websites which I do not trust. The reason for this is that you know that newsletters and stuff like that come in. And it's not on ... I have a work email and then I have another email, which I never use for those profiles. So, I have one just set up for that… (Younger group, lower education, IP2).

In this way, the participant creates a sort of alter ego and thereby displaces the risk or annoyance she feels to an alternative email inbox. Similar to this, a minimizing coping strategy was to outsource the risk-taking to others. One participant completely relied on her husband's internet setup and security settings, but still complained that she felt exposed and worried, because they had security cameras installed everywhere in the house. Another participant similarly felt less at risk because his workplace had "high security". In this way, minimizing risk means that the participants avoided data anxieties because they transferred the responsibility to other people whom they felt were more knowledgeable and capable than themselves. As we see, both the disconnection strategy and the minimizing strategy are linked to an absence of trust in the digital platforms and their capabilities to protect the data. But we also see that disconnection and non-usage are chosen as tactics where the participants do not feel dependent—for example, if work or school somehow forces them to have a profile on Facebook. The third tactic is, in contrast, linked to actively choosing to trust.

Coping by trust

Coping by trust came in many forms but was most often mentioned in relation to platforms of a certain size. The argument seemed to be, on the one hand, that if the platform is of a certain size, like Facebook, then it will have so much of people's data that it will be able to protect it. On the other hand, trust was often the chosen coping strategy when platforms connected to state ownership, such as tax, health or apps connected to education, were discussed, as everyone agreed that the data were much more sensitive (i.e. personal) and that these platforms could not be avoided. These platforms and services were described in a much more positive manner, and possible data mining was accepted by and large as it could "help society"—for example, by detecting diseases or families with problems. This participant explains why she is not worried about the data traces she leaves on platforms owned by the government:

> I think that's because it is the government who is sending the information. And okay, it may well be that they collect our data for something, but I don't think there's an unethical

> purpose behind it. So, they also have all my personal information already, so, what else do they want to know? How often I open my e-box (a nationally created platform for receiving e-mails from the public sector)? I don't mind them knowing that (Older group, higher education, IP2).

Again, we see the participant negotiating the risk in the type of data given to the platform and the level of faith in the authorities not to use these data for unethical purposes, though without specifying what such purposes might be. Along the same lines, we saw how the participants used past experiences as a point of reference. This was in both positive and negative terms—either "I have never experienced that they have used my data in ways that I did not expect them to" or "I heard this about the data leak, so I did this…". These past experiences also relied on the specific relationship with platforms, such as the school or the bank, which were seen as institutions that could be trusted because they also had an interest in maintaining a good relationship. As this participant describes:

> And I want to say, as far as online banking is concerned, we are already in an offline dialogue with them about our finances, you have to have a loan, or your child's savings and so on. And then, I would say that it is a sort of relationship of trust that you have entered into with your bank, and therefore I trust that they use my data, but it is also a cooperation, which I myself have agreed to (Older group, short education, IP2).

Coping by apathy

We have chosen to name the last of the coping tactics that we found in the material 'coping by apathy'. It involves the participants shrugging it off, but in two different ways, or for two different reasons. Some participants were reluctant to accept that the risk noted by other participants, existed, mostly because they did not think the data were sensitive or because it even was an advantage to engage with these services, which would come to know them and, for example, give them better film recommendations.

> I am not too scared about it floating around the web—well, then, you have my personal number. What can they use it for? They can use it to scam something, but I think about insurance more often. Do I have the option of replacing things if this happens? (Older group, higher education, IP3).

> I would say, if they have my email or login, they could threaten me, but they cannot threaten me with my preferences in films (Younger group, lower education, IP4).

As the quotes show, these participants are not so worried about film preferences or even their personal number being online unless the data are being used for swindling or similar. Others, though, were much more worried—however, again distinguishing between the platforms or services, indicating that Facebook is not a platform to trust with any sensitive data:

> If they [Facebook] track my messages, it wouldn't surprise me that they do. So, they are not very exciting, my messages, but I have no confidence. I would not write my CPR number or bank details. I would never write that in Messenger (Older group, lower education, IP5).

Apathy also involves imagining the worst case, even though, as this participant expresses, his knowledge is insufficient and he has no way of finding out if Facebook is tracing his Messenger. So, it helps him to imagine that they do, emphasizing that he does not care that they "listen in", except if they get access to his personal number. But apathy as a coping tactic could also be seen when participants actually felt at risk but nevertheless felt unable to do anything about it. Hence, we found a form of acceptance of the complexities, as the participants become aware that the little room for minimizing risk is likely to be insufficient to cover their data traces. This is, of course, linked to the "feeling of powerlessness" found by Andrejevic (2014, p. 1675) and the "surveillance realism" found by Dencik and Cable (2017, p. 764). As this participant expresses, it is simply too hard to be worried all the time:

> I simply reach some point where I say that if I am so scared then I cannot use these platforms. I can simply no longer accommodate. So, I have to be an optimist, and then I have to be happy and a little naive and say that: 'Yes, I am as careful as I possibly can be ... '(Older group, higher education, IP4).

Contextual factors: A coping compass for navigating the data anxieties

Above, we have seen complex negotiations of how to navigate the data anxieties, but two important contextual factors emerged in the material. We argue that many of the digital services and platforms that were mentioned by the participants differ in terms of how dependent the participants are on these platforms. Being dependent is also relational, however, and while some participants might feel dependent on Facebook, others might not. The other contextual factor that comes into play is the risk evaluation, as pointed out by Hargittai and Marwick (2016), in that the participants weigh the pros and cons—more specifically, they evaluate the risk according to the type of data and the type of platform they are engaging with. As such, if you perceive the platform to be high risk, you will attend to the sort of data you feel comfortable giving the platform, whereas this evaluation becomes less important if the data are non-sensitive to the participants, such as their shoe size or film preferences. The important thing is that if the participants at times evaluated the platform as a combination of being of low trust and the data non-sensitive, then they would either try to minimize or shrug their shoulders. These evaluations and the coping tactics chosen are illustrated in Figure 1, the coping compass.

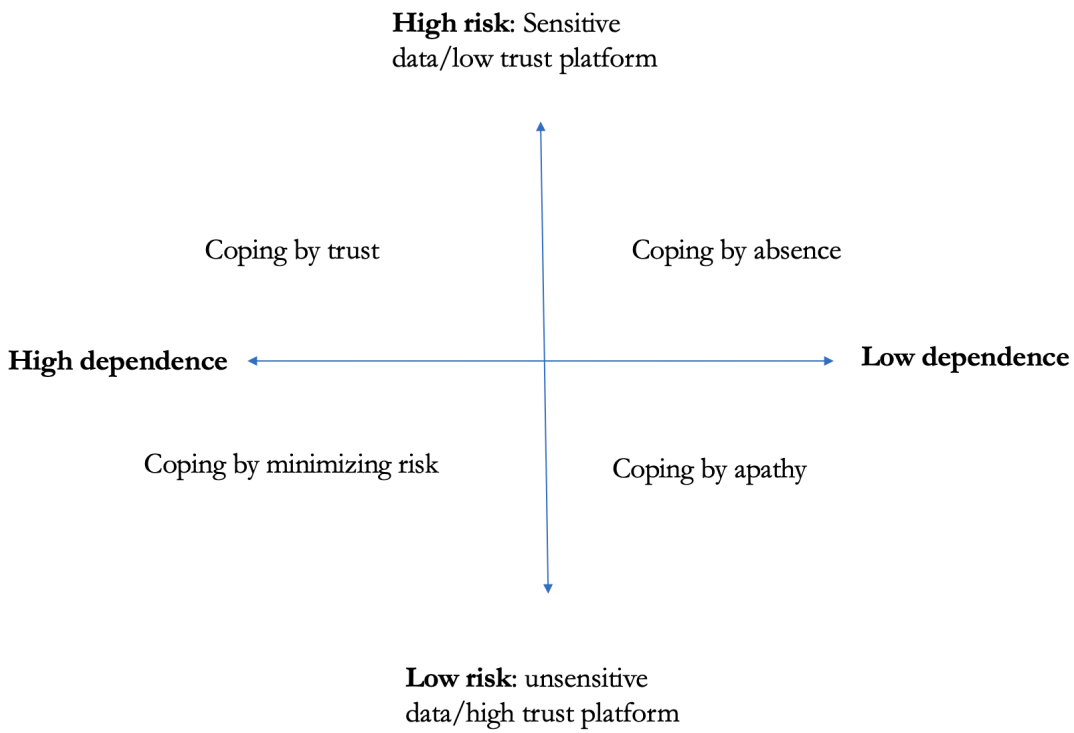

Figure 1. The compass of coping tactics in datafied everyday life

The compass enables an analysis of individual users and their coping tactics in relation to specific digital platforms and apps, moving from left to right or up and down on the continuum of dependence coping and the continuum of risk coping.

In the upper left quadrant, we found the participants often only chose trust as a tactic when they were dependent on the platform, such as a school app or the nationally created app and platform for receiving letters from public authorities (named E-box). They did not necessarily perceive these platforms as high risk, but the data they contained were often mentioned as high risk. Similarly to Pink et al. (2018), we found that trust was coherent with a focus on process, emergence and (im)possible rather than predictable futures. This therefore involves approaching the concept of trust as a feeling that specifically refers to the ability to be able to move on and do something in the immediate future. It need not involve absolute certainty, but entails feeling and knowing enough to be able to take the next step. Trust, as Pink et al. (2018) argue, is the moment in which we feel sufficiently confident to be able to act, whereby "confidence based on familiarity is the foundation of getting involved in a situation" and differentiates trust from risk (Fredricksen, 2016, p. 59, in Pink et al., 2018, p.3). We found, though, that risk is very much involved in the participants' abilities to trust in the immediate future, and that trust is often a necessity related to the fact that the participants are dependent on the platforms that they choose to trust. However, dependence is also understood here as a 'feeling' which emerges from the

discussion of whether one could actually function in a digital society without using many such platforms: for some, it would just require too much work to choose disconnection as a tactic, even though it would be possible, in theory at least.

In the bottom right corner, the tactic of apathy was employed when users felt little or no dependence of the platform and perceived little risk by the usage. For example, platforms like Netflix or the shopping site Zalando were met by a tactic of apathy, as many of the participants did not see film preferences or shoe sizes as high-risk data.

Equally, Messenger was mentioned in relation to the 'shrugging' done by participants. It can seem like a paradox that users engage with platforms that they openly do not trust, but here we saw the response of apathy, often because the data was considered non-sensitive, therefore making trust irrelevant despite the fact that the participants saw what they wrote in Messenger as private. This became apparent in the way the participants distinguished between using Facebook and Messenger, essentially the same platform, but Messenger was by many seen as less risky than Facebook. Hence, when the participants felt they could not trust—i.e. were sufficiently confident to act but were still dependent on usage of the platform—they engaged in apathy as a tactic, questioning whether Facebook is listening in on their Messenger conversations, but being okay about it or downplaying the riskiness because, as one participant explained: "it's only for advertising", or, as another said: "it's only gossip between me and my friends".

In the upper right quadrant of the compass, we found the tactic of disconnection employed, when users were aware of the risk, either of the type of data or the type of platform, but were not dependent on using the platform. These were platforms such as weather apps, health apps or, for some, even Facebook. For some, the data they produce by using the platform is sensitive, like a menstruation cycle, while for others disconnection was not about the type of data but about past experiences and discourses around the platform as high risk.

Conclusion

Previous research has identified a "privacy paradox" (Young & Quan-Haase, 2013), showing that users engage in a calculation weighing the pros and cons of online media use in order to justify their everyday use and dependence on platforms such as social network sites (Hargittai & Marwick, 2016). Furthermore, research on everyday datafication often suggests the user as anxious (Pink et al., 2018), powerless (Andrejevic, 2014) or with "feelings of widespread resignation" (Dencik & Cable, 2017, p. 773).

Our article has departed from this by exploring coping beyond social media to include platforms and apps such as banking, health and shopping, and by focusing on what Pink et al. (2018) have conceptualized as mundane data routines and habits of coping with data anxieties, and thus ordinary users' coping strategies. This has enabled us to see how these negotiations are always complex and relational. The framework of algorithmic

delegation (Willson, 2017) and user tactics of resistance (de Certeau, 1988) directed our gaze towards coping tactics as productive practices and towards the contextual factors, illustrated analytically in the coping compass.

By taking a bottom-up approach, following Kennedy et al. (2015) when they encourage research to "attend to diverse, individual and subjective responses to everyday tracking" (p. 3), this article has identified four types of coping tactic, namely coping by disconnection, coping by trust, coping by minimizing risk and coping by apathy. While disconnection is often chosen when the participants evaluate their dependence on the platform as low and the cons outweigh the pros, minimizing includes tactics such as not posting, lurking, turning off the camera or geo-location.

We have observed how many of the everyday tactics are not as tactical or strategic as the name indicates, but are often about maintaining the flow of everyday life without being disturbed by the so-called chilling effects, for example, Google Maps knowing that you are likely to drive to work in the morning and how long it will take you to drive there.

Thus, we see the investment has to fit the result, and when feeling at risk participants try to "imagine an immediate future" (Pink et al., 2018, p. 3) and hope that it is enough to feel safe.

Similarly to Kennedy et al. (2017) we saw differences between young and old, and between educated and less educated, although our data cannot be generalized. It remains an important question to examine whether people of different ages and backgrounds perceive risk and dependence in different ways, or if similar coping tactics can be found in similar groups.

Andrejevic (2014) conceptualizes the asymmetry between the knowledge held by big data companies and the lack thereof amongst ordinary people as a "big data divide", leaving people with an "expressed sense of powerlessness vis-à-vis the arrangements that structure the collection and use of personal information" (p. 1682). Future research could study such divides within user groups, in terms of usage of platforms and links to the data anxiety experienced by those users. The question is on the one hand how data anxiety and coping are ingrained in discourses of datafication and a result of increased complexity through datafication? And on the other hand how the intrusiveness of digital platforms in people's everyday lives is making it almost impossible to imagine other futures or even to begin to grasp how disconnection could be an option. In other words, how can users minimize the future risk of datafication in a present that they do not fully understand?

References

Andrejevic, M. (2014). The big data divide. *International Journal of Communication*. 11, 1673-1689. https://doi.org/1932–8036/20140005

Barbour, R., & Kitzinger, J. (1999). Introduction: The challenge and promise of focus groups. In J. Kitzinger & R.S. Barbour (Eds.), *Developing focus group research* (pp. 1–20). London: SAGE. https://doi.org/10.4135/9781849208857.n1

Bloor, M., Frankland, J., Thomas, M., & Robson, K. (2012). *Focus groups in social research*. London: SAGE. https://doi.org/10.4135/9781849209175

Bolin, G., & Andersson Schwarz, J. (2015). Heuristics of the algorithm: Big data, user interpretation and institutional translation. *Big Data & Society*, *December 2*(2), 1–12. https://doi.org/10.1177/2053951715608406

Bottis, M., & Bouchagiar, G. (2018). Personal data v. big data in the EU: Control lost, discrimination found. *Open Journal of Philosophy*, *8*, 192–205. https://doi.org/10.4236/ojpp.2018.83014

Cate, F.H., & Mayer-Schonberger, V. (2013). Notice and consent in a world of big data. International Data Privacy Law, 3(2), 67-73. *International Data Privacy Law*. https://doi.org/10.1093/idpl/ipt005

Couldry, N., & Mejias, U.A. (2018). Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject. *Television and New Media*. 20(4), 336-349. https://doi.org/10.1177/1527476418796632

Crawford, K., & Schultz, J. (2014). Big data and due process: Toward a framework to redress predictive privacy harms. *Boston College Law Review*, *55*(93), 93-128.

de Certeau, M. (1988). The practice of everyday life: 'making do': Uses and tactics. In G.M. Spiegel (Ed.), *Practicing history: New directions in historical writing after the linguistic turn* (pp. 217-227). New York: Routledge. https://doi.org/10.4324/9780203335697

Dencik, L., & Cable, J. (2017). The advent of surveillance realism: Public opinion and activist responses to the Snowden leaks. *International Journal of Communication*, *11*, 763–781.

Dencik, L., Hintz, A., & Carey, Z. (2018). Prediction, pre-emption and limits to dissent: Social media and big data uses for policing protests in the United Kingdom. *New Media and Society*, 20(4), 1433 –1450. https://doi.org/10.1177/1461444817697722

Draper, N.A., & Turow, J. (2019). The corporate cultivation of digital resignation. *New Media and Society*, 21(8), 1824-1839. https://doi.org/10.1177/1461444819833331

Frederiksen, M. (2016). Divided uncertainty: A phenomenology of trust, risk and confidence. In S. Jagd & F.L (Eds.), *Trust, Organizations and Social Interaction: Studying Trust as Process within and between Organizations* (pp. 43-67). https://doi.org/10.4337/9781783476206.00011

Gerber, N., Gerber, P., & Volkamer, M. (2018). Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers and Security*, 77, 226-261. https://doi.org/10.1016/j.cose.2018.04.002

Gray, J., Gerlitz, C., & Bounegru, L. (2018). Data infrastructure literacy. *Big Data and Society* 5 (2). https://doi.org/10.1177/2053951718786316

Hargittai, E., & Marwick, A. (2016). 'What can I really do?' Explaining the privacy paradox with online apathy. *International Journal of Communication*, 10(2016), 3737-3757. https://doi.org/10.5167/uzh-148157

Kennedy, H. (2018). Living with data: Aligning data studies and data activism through a focus on everyday experiences of datafication. *Krisis: Journal for Contemporary Philosophy*, *1*.

Kennedy, H., Elgesem, D., & Miguel, C. (2017). On fairness: User perspectives on social media data mining. *Convergence* 23 (3). https://doi.org/10.1177/1354856515592507

Kitzinger, J. (1994). The methodology of focus groups: The importance of interaction between research participants. *Sociology of Health & Illness* 16(1). https://doi.org/10.1111/1467-9566.ep11347023

Latour, B., & Johnson, J. (1998). Mixing humans and nonhumans together: The sociology of a door-closer. *Social Problems*, *35*(3), 298–310. https://doi.org/10.1525/sp.1988.35.3.03a00070

Mayer-Schönberger, V., & Cukier, K. (2013). *Big Data: A Revolution That Will Transform How We Live, Work and Think*. New York: Houghton Miffl in Harcourt. https://doi.org/10.3359/oz1314047

Millington, B., & Millington, R. (2015). 'The datafication of everything': Toward a sociology of sport and big data. *Sociology of Sport Journal 32*(2). https://doi.org/10.1123/ssj.2014-0069

Newman, N., Levy, D.A.L., & Nielsen, R.K. (2018). Reuters Institute Digital News Report 2018. *University of Oxford*. https://doi.org/10.1017/CBO9781107415324.004

OECD. (2019). *OECD Economic Surveys - Denmark*.

Pangrazio, L., & Selwyn, N. (2018). 'Personal data literacies': A critical literacies approach to enhancing understandings of personal digital data. *New Media & Society* 21(2). https://doi.org/10.1177/1461444818799523

Picone, I., Kleut, J., Pavlíčková, T., Romic, B., Møller Hartley, J., & De Ridder, S. (2019). Small acts of engagement: Reconnecting productive audience practices with everyday agency. *New Media and Society* 21(9). https://doi.org/10.1177/1461444819837569

Pink, S., Lanzeni, D., & Horst, H. (2018). Data anxieties: Finding trust in everyday digital mess. *Big Data & Society*, *January* 5(1), 1–14. https://doi.org/10.1177/2053951718756685

Ruckenstein, M., & Schüll, N.D. (2017). The datafication of health. *Annual Review of Anthropology*, *46*(1), 261-278. https://doi.org/10.1146/annurev-anthro-102116-041244

Smith, G.J.D., & O'Malley, P. (2017). Driving politics: Data-driven governance and resistance. *British Journal of Criminology 57*(2), 275–298. https://doi.org/10.1093/bjc/azw075

Sumartojo, S., Pink, S., Lupton, D., & LaBond, C.H. (2016). The affective intensities of datafied space. *Emotion, Space and Society*, 21, 33-40.. https://doi.org/10.1016/j.emospa.2016.10.004

van Dijck, J. (2014). Datafication, dataism and dataveillance: Big data between scientific paradigm and ideology. *Surveillance and Society*, *12*(2), 197–208. https://doi.org/10.24908/ss.v12i2.4776

Willson, M. (2017). Algorithms (and the) everyday. *Information Communication and Society 20*(1)*,* 137-150. https://doi.org/10.1080/1369118X.2016.1200645

Young, A.L., & Quan-Haase, A. (2013). Privacy protection strategies on Facebook: The Internet privacy paradox revisited. *Information Communication and Society. 16*(4), 479-500. https://doi.org/10.1080/1369118X.2013.777757

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. New York: PublicAffairs. https://doi.org/10.4000/qds.3723

Jannie Møller Hartley
Department of Communication and Arts
Roskilde University

Sander Andreas Schwartz
Department of Communication and Arts
Roskilde University