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

Article – Theme section

Appscapes in Everyday Life
Studying Mobile Datafication from an Infrastructural User Perspective

Signe Sophus Lai and Sofie Flensburg

MedieKultur 2020, 69, 29-51

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

It has long been acknowledged that the use of 'free' mobile apps comes at a price, but few empirical studies have looked into this supposed trade-off. This article combines qualitative interviews with mappings of infrastructures for datafication in order to study the implications of mobile app usage from the perspective of individual users. It analyses users' understanding of online tracking, maps the infrastructural tenets of mobile datafication, and finds a disconnect between what users believe happens to their data and the actual data harvesting and distribution mechanisms of their apps. We thereby argue that users' resigned attitudes should be understood in light of the material conditions of the app economy and, as such, that user and infrastructure studies should join forces in exploring and enhancing users' agency, empowerment and emancipation.

Keywords

Infrastructure, apps, datafication, digital resignation, data economy, surveillance

Introduction

Smartphones are now an integral part of most people's everyday lives. However, mobile apps' data collection methods and the distribution and use of mobile meta data are still far from common knowledge to users and scholars (for exceptions, see Atkinson et al., 2015; Binns et al., 2018). While user studies have looked into people's "algorithmic imaginaries" (Bucher, 2017) and have identified a "privacy paradox" separating users' opinions from their actions (Barth & de Jong, 2017), few studies have mapped how data actually flow from individual users' smartphones (Lai & Flensburg, 2020) and none have, to the best of our knowledge, combined inquiries into user attitudes towards online tracking with an exploration of the infrastructural mechanisms of mobile datafication. This article therefore introduces a novel approach to the critical interrogation of datafication by combining a user-centric focus with broader macro perspectives that emphasize material infrastructures and business models as structuring forces that shape the everyday lives of regular smartphone users.

Building on current scholarly discussions of the implications of datafication in terms of commodification of users (Couldry & Yu, 2018) and data (in)justices (Dencik et al., 2019), we argue, on the one hand, for the advantages of an infrastructural turn (Musiani et al., 2016) in user studies that focus on the political economy of data harvesting and tracking. Infrastructure studies, on the other hand, can benefit from applying a user perspective when scrutinizing the data economy's opaque business models and obfuscation practices (Draper & Turow, 2019). By combining insights into users' experiences and understanding of online tracking with knowledge on the infrastructural mechanisms of apps, we are able to produce a more coherent and nuanced understanding of user agency and possible ways to enhance it through, for instance, regulatory interventions.

In the following, in order to contribute to existing studies on how datafication impacts the everyday lives of smartphone users, we explore how user and infrastructure studies, as two separate strands of research, can be combined and mutually inform one another. The article first analyses 20 regular smartphone users' understanding of datafication and online tracking, and then maps how the different apps installed on individual users' phones result in different types and degrees of data harvesting and distribution. We thereby develop what we have termed the 'appscape' approach (Lai & Flensburg, 2020) in order to engage empirically with the implications of commercial mobile infrastructures for individual users, and to offer a tool whereby these implications can be made transparent and accessible to researchers and users alike.

The article consists of four main sections. In the first, we present the theoretical foundations for the article and argue that the appscape approach represents a novel contribution to critical data studies and the emergent field of app studies by applying a human-centred but technologically-informed approach to uncovering the datafication of everyday life. The second section presents the methods and empirical material, emphasizing the value of combining thick interview data with mappings of infrastructures for

datafication. The third part presents the two analyses, respectively of the respondents' understanding of datafication and online tracking, and of their individual appscapes. The fourth and concluding section discusses how this approach can ground future studies, consumer campaigns, and regulatory interventions.

Literature review and theory

We position our research in the broad field of critical data studies (Dalton & Thatcher, 2014) that, in recent years, has pushed a critical agenda on the ubiquitous datafication (Mayer-Schönberger & Cukier, 2013) of everyday life and challenged the hype surrounding big data (boyd & Crawford, 2011). The field has, in particular, contributed with theoretical insights and conceptual work on what big data means (e.g. Kitchin, 2013), central research areas and questions (e.g. Dalton & Thatcher, 2014), and encouragement for research to empower and mobilize users (e.g. Iliadis & Russo, 2016). However, consistent calls have been made for more "empirical research to underpin and flesh out critical data studies" (Kitchin & Lauriault, 2018, p. 18). Two related, but separate, strands of research have answered this call through empirical analyses of the consequences of datafication. User-oriented studies with a particular focus on privacy have explored individual internet users' capacity to understand and their ability to actively opt out of digital data harvesting (e.g. Barth & de Jong, 2017), while digital infrastructure studies (Sandvig, 2013) have uncovered the materiality (Winseck, 2019) and ownership of digital infrastructures underlying the abundant data economy (Zuboff, 2019). The following sections give a brief account of existing research in each field and conclude by defining the concept of the appscape as an epistemological and methodological tool for combining the two traditions in empirical analyses.

Users' experiences with datafication: Privacy concerns and resignation

Studies of datafication and everyday life usually build on interviews or other qualitative research designs in order to uncover how digital media users understand and cope with online tracking, algorithms, and so forth (Bucher, 2017; Dubois & Ford, 2015; Kennedy & Hill, 2017). Among the most prominent and well-documented findings is the so-called privacy paradox (Barth & de Jong, 2017) that identifies a discrepancy between users' attitudes and behaviours towards protecting their data. The paradox implies that knowledge and awareness of privacy risks do not necessarily lead to more restrictive or critical behaviours (Joinson et al., 2010; Oomen & Leenes, 2008; Pötzsch, 2009). The paradox has been explained in different ways. Some argue that users' strategies build on rational calculations, where the disclosure of data is seen as a reasonable price for a desired product (Acquisti & Grossklags, 2005). Others argue that users tend to underestimate the actual implications of their digital activities (Norberg et al., 2007) and instead focus their attention on deliberate data disclosures (what information they choose to register

or publish), with far less concern for the harvesting of meta data (through, for example, cookies, mobile permissions, etc.) (Young & Quan-Haase, 2013). Common to these studies is an underlying premise of a (more or less conscious) trade-off between the user and the provider of a given service. Irrespective of whether or not the user understands the fundamental conditions and the 'price' required by the supplier, the service in question is assumingly making it worth it (Barth & de Jong, 2017).

Draper and Turow (2019), in turn, dismiss the idea of an actual trade-off. Referring to the "trade-off fallacy" (p. 1825), they argue that users are caught in the terms and conditions put up by the digital service providers and are de facto unable to opt out. The users' attitudes are thus not all that paradoxical but rather a result of resignation: "[…] while these people feel dissatisfied with the pervasive monitoring that characterizes contemporary digital spaces, they are convinced that such surveillance is inescapable" (ibid.). Draper and Turow (2019) further argue that resignation to datafication follows not only from the seeming inevitability of data harvesting but also from a deliberate market strategy revolving around corporate obfuscation (Ellison & Ellison, 2009). That is, companies that make a living from collecting, processing or selling user data have a commercial interest in creating obstacles (like endless pages of terms of service, hardwired functionalities, etc.). These obstacles discourage users from taking action towards protecting their data and serve to black box tracking activities further, thereby avoiding consumer complaints, political debate and regulatory interventions. In line with this argument, user understanding should not only be seen as something that is shaped in the minds of individual users, but also as framed by the infrastructural and economic conditions that structure mobile communication.

Apps as infrastructures

Digital infrastructure studies seek to uncover the material foundation for datafication and to explain the corporate practices and power structures that are built into digital technologies. This includes studies that reverse-engineer web tracking systems and expose the depth and extent of datafication (Falahrastegar et al., 2014; Kalavri et al., 2016), as well as analyses of how different material components of the internet infrastructure are controlled and governed (Galloway, 2004; Musiani et al., 2016; Sandvig, 2013; Winseck, 2019). In the field of app studies, the infrastructural approach has been applied in studies of how individual apps collect and distribute data (Nieborg & Helmond, 2018; Weltevrede & Jansen, 2019), while computer scientists have mapped out entire mobile tracker ecosystems (Binns et al., 2018; Vallina-Rodriguez et al., 2016). These studies provide valuable knowledge on app infrastructures and business models, but often neglect to ask how these infrastructure and market configurations impact ordinary users whose lives are so dependent on them.

In the following analysis, we recast the users as part of the equation by emphasizing the ways in which the infrastructural arrangements of the app economy frame and condi-

tion users' digital agency. From an infrastructural perspective, users' abilities to understand and control data harvesting and distribution are closely linked to the infrastructural architecture of smartphones and apps. As more and more of what counts as social life is lived through mobile technologies and applications, the need for studies that scrutinize the principles of this architecture only increases. As such, the infrastructural approach holds a sensitizing potential in that it recalls "the simple crucial fact that each communication technology is a material resource whose distinctive features help to explain the [...] the communicative practices that have emerged, or which may emerge in the future" (Jensen, 2013, p. 216). This does not mean that it is unimportant what people say and do with these technologies, but rather that we should ground studies of user agency in the material conditions of their everyday communications. The approach suggested in this article therefore explores the macro structures that frame individual app use from a micro perspective—namely that of appscapes.

The concept of appscapes epitomizes the merger of macro-oriented studies of infrastructures and micro-oriented studies of users' understanding of online tracking and establishes a middle-ground for studying the implications of mobile datafication. It is motivated by a desire to map the landscape of mobile surveillance as seen from the perspective of the individual smartphone user. We thereby take the agency of and diversity between smartphone users into account, while at the same time considering mobile data harvesting and distribution as rooted in and shaped by the greater app infrastructures and the market actors who control them. In other words, we focus on, and talk to, users, and go on to situate their mobile communication in the greater app environment.

The appscape approach: Methods and data sources

The appscape approach is developed on the basis of a multi-sited ethnographic fieldwork study (Marcus, 1995) of the role of the internet in everyday life, carried out in early 2018 in Denmark (Lai et al., 2019). The next sections will outline the basic principles of this fieldwork and the data it produced, as well as the ways it motivated the development of the appscape approach as a necessary next step towards understanding and explaining how mobile datafication impacts users' everyday lives.

Qualitative interviews and user understandings

The ethnographic study combined maximum variation and network sampling in order to produce an interview sample of 20 individuals. As a result, the respondents are diverse in terms of age, gender, place of residence and household, ethnicity, educational level, religious beliefs, and relationship and parental status. They thereby make up a broad sample of the adult Danish population: they use the internet—and smartphones in particular—in very different ways, have installed different apps, and exhibit different levels of digital knowledge, skills and resources. This sampling strategy enables deep descriptions of the

individual cases, shows diversity between them, and highlights patterns across seemingly different groups of people (Patton, 2015).

The interviews were semi-structured (Brinkmann & Kvale, 2009), following an interview guide that featured general questions about people's everyday lives and more specific questions surrounding their communication activities, including aspects of datafication and tracking. All interviews were transcribed; transcripts were fully anonymized (names of respondents, places of residence and work, and names of close relations), and the respondents were given pseudonyms. The transcripts were then subjected to thematic analysis (King & Horrocks, 2010), which entailed consensual and iterative coding by the authors of the sections of the interviews where the respondents talked about their data streams, targeted advertisements and so forth. The initial descriptive coding returned a multitude of codes, like 'feelings of not knowing what is going on', and gave rise to a continued redefinition of the codes. Next, interpretive coding clustered the descriptive codes in relation to the research question, and the interpretive codes, like 'loss of control', were applied to the material. Lastly, overarching themes, like 'control', were derived from the interpretive and descriptive codes by returning to the theoretical underpinnings of resignation and obfuscation.

While the interviews led us to interesting observations that to a large extent confirmed established notions around digital resignation, they also had us wondering what the underlying premises were for the respondents' experiences and understanding: how and with what implications were their everyday lives tracked, monitored and commodified through their particular configuration of apps? And how did this relate to—or not relate to—their own understanding? Upon realizing this, we reached the conclusion that their understanding alone was insufficient to explain the impact that datafication had on their lives. In other words, motivated by the empirical aim of understanding the agency of individual smartphone users, we decided to combine the user study described above with an infrastructural approach to datafication.

Mapping app permissions and third parties

As part of the initial interview, the respondents guided walkthroughs (Light et al., 2018) of their individual smartphones, and some of them took screenshots of their home screens from which we were able to deduce the apps that were downloaded to their phones (hereafter referred to as the participants' individual app repertoires). The walkthrough manoeuvre amounted to a total of 173 unique apps distributed across a total of ten respondents. Some apps were shared by all ten, who each had between 11 and 62 downloaded apps on their smartphones, and some were unique to just one of them. Given the lack of any official or public databases containing information on the most used apps, the dataset in this article creates a valuable, though not representative, sample of common and generally used apps in Denmark as well as lesser known ones down the long tail of existing apps (Lai & Flensburg, 2020).

To gauge the intrusiveness of the different apps, we used as empirical indicators the number and types of accesses and permissions requested by the individual app, as well as the different third-party services it communicates data to. An app's accesses and permissions offer insights into the types of meta data that are available to the app, granted by the user upon installation. The app's embedded third-party services, in turn, relay information on the extent to which the app's data can be shared, as well as the kinds of actors that harvest and use the data. While some permissions can be declined or changed later in the phone settings, for the purpose of this analysis we focus on the default settings of the apps in question—that is, the respondents could in principle have altered these settings, but the interviews did not indicate that this was the case. The data were obtained through scraping the Google Play Store in February 2020 for information (price, rating, category, etc.) on each app, as well as its requested accesses (e.g. location, pictures/media/files, SMS) and permissions (e.g. precise location [(GPS & network-based], modify or delete the contents of your USB storage, read your text messages [SMS or MMS]). The scrape returned a total of 115 unique permissions distributed across 15 overall types of access. While some permissions are foundational for the functioning of the particular app (however, only when the apps are used), others are strictly for user commodification and data monetization purposes: flashlight apps, requesting more than 70 permissions that have nothing to do with the specific functionality of a flashlight, are extreme cases of this (Cimpanu, 2019).

Much like cookie scripts in websites, apps can implement third-party services in small pieces of software, often distributed by companies in ready-made toolkits (so-called software development kits, or SDKs). The third-party services connected to the 173 apps, extracted from the source codes of the apps, were obtained through the Exodus database (n.d.), also in February 2020. This returned a total of 107 unique third-party services (e.g. Branch Metrics or Umeng Analytics), owned by 88 different parent companies (e.g. Branch or Alibaba), and offering different services (e.g. running analytics, serving ads). Google Play Store is the default platform for these types of research interventions (Binns et al., 2018; Exodus, n.d.), yet it also comes with a number of important limitations. Most significantly to this article, the dataset reflects the Google Play Store at the time of the scraping, as well as the standing Android operating system (OS) (the Android 10 release): as such, it cannot reflect differences across Android and iOS, app stores or OSs. This specific methodological constellation therefore does not allow for a precise reproduction of the individual respondents' empirical reality, which is, of course, a lot more complicated: they owned devices running both Android and Apple OSs; some of them had not updated their software for months, and even if they had, this was back in 2018. This is, however, a necessary evil in the emergent app studies field, where data move fast and analyses will inescapably always reflect a particular point in time.

To sum up, smartphone users' individual appscapes are made up from their particular constellations of apps, the accesses and permissions requested by the apps, and the

third parties they cooperate with. As described above, the appscape analysis was not part of the initial research design, but served as an explorative endeavour to explain and substantiate the findings from the interviews. In other words, it represents a first effort at uncovering the underlying data infrastructures that ground individuals' app usage and their experiences of datafication. Future studies should employ and develop the method in order to produce more coherent empirical work in the nascent field of app studies (Nieborg & Helmond, 2018).

Interview analysis

In the following, the thematic interview analysis is summarized in four common responses to online tracking. The four themes are interrelated and fluid, and can be collected under the headlines of: "It's scary", "I have nothing to hide", "As long as it's relevant", and "Free is a good price". As ways of understanding or coping with the increasing datafication of everyday life, the themes offer four ways in which digital resignation (Draper & Turow, 2019) is articulated and lived out in everyday life. The analysis shows the relationships between the themes and the interview material, but also how the respondents traverse and cut across the four responses over the course of their interviews.

'It's scary'

One of the most common statements whenever conversation touched upon targeted ads in apps like Facebook, Google Search, Candy Crush or any other app financed through in-app advertising, can be boiled down to, as Fatma, a 25-year-old teacher, puts it: "I just think it's scary". Usually statements like Fatma's were followed in the conversations by different examples of how this scariness had played out in mundane situations. For instance, Johnny, an employed consultant in his 30s, described how Google used to send him push notifications on his Android phone which were based on his routines and whereabouts:

> If you take the same route enough times, then it comes up and says 'This train is delayed', 'This train is not delayed'—that's Google+. But of course it's something you can turn off somehow, it's a settings thing, but I never really [...] I think it's scary because it turns into a bigger and bigger overview over what we're doing.

In the quote, Johnny explains how he is aware that this particular feature of the smartphone could perhaps be switched off somewhere in the phone settings, and even though he clearly thought about it and was bothered by the constant notifications, he never took the actual steps to reconfigure the default phone settings. In a different conversation, Hanne, a 22-year-old real estate intern, described how, even if she were determined to alter the settings so as to block, in her case, location-based tracking, she would not know where to start:

> Actually today, I think it was on Instagram, two of my colleagues were suggested, where I thought, okay I was just at work yesterday, where they were, and I think that's kinda scary that … I don't know if [the app] registered that we were close to each other and then they're suggested [...] I think it's creepy, but I don't do anything about it and I actually also don't know how I should do it, because I think it's really difficult to shut down everything when you have so many apps, so I wouldn't know where to begin.

Hanne was asked, what it would take for her to take action towards protecting her location data, and she replied: "I really don't know—perhaps if you get a sick stalker or (laughs)… I don't know; as things are now, I don't think I'll do anything about it, because that's just the way it is, I think". In this quote, Hanne highlights how the threat of another person is much less abstract than the stalking carried out by an app like Instagram. She also emphasizes two other common features across the interviews, which is the absence of proper knowledge on what to do and the general naturalization of commercial tracking, in which corporate power over data is viewed as an "inevitable and immovable feature of contemporary life" (Draper & Turow, 2019, p. 1829).

'I have nothing to hide'

The second common statement in the interview material focuses on how trying to counter online tracking might give the impression that one has something to hide. Sofia, a 28-year-old occupational therapist, first articulated a fear similar to the one described above when talking about personalized ads in her feed and her own responsibilities: "you become a bit scared, because you start thinking about how much you're giving permission to, because it is... I'm the one giving permission to it, but how and, like, when did I do that?" As the conversation continued, she emphasized the normalcy of it, however, explaining why she was not all that worried about data collected on her online activities:

> Sofia: You're both a bit nervous but then I also think, 'okay, what could happen' or... if you don't have anything to hide.
> Interviewer: Yes, like, so what if Facebook knows that I searched for jumpsuits?
> Sofia: Yes, exactly! But it's still not comfortable [Interviewer: No]… of course you'd rather it wasn't there, but now it's, like, at first I thought it was a bit infringing, now it's more normal [...] I think it's something about getting used to it.

Kai, an 85-year-old retiree, put it more bluntly than Sofia: "Personally I don't give a damn, because I don't do anything online that I couldn't put out there in public and I can't, I can't imagine that, eh, that there's anyone who could get anything out of surveilling me at all." Tim, a priest in his 50s, expressed a similar attitude, explaining that he was indeed afraid if maybe the large sums of data collected about people could one day be used to control them, yet he did not fear for himself:

> I'm not doing all that many things that are (laughs) are worth looking for or storing [...] I mean, I don't think that I, as a person, am that important (laughs) in that way, it's not myself I'm scared for, it more the... the big masses' use of it, right [...] If I'm buying something [online], then I think, it'll probably be alright, because I want that thing, even though (laugh) it doesn't look totally safe.

The quote from Tim articulates a general concern for the population or the world as a whole, but a lack of concern for oneself, perhaps, as Tim also hints, because the need or desire to obtain a given service through a certain app overrides the concerns.

'As long as it's relevant'

A third common response can be summarized under a headline of relevance. For instance, Liam, a 52-year-old factory worker, explained that he hated when online ads for something he had already bought (in this case, a flight to a European country) kept coming up again and again. He also said resignedly, however, that this is an unavoidable feature of online shopping.

Elaborating on the view that ads can be a welcome distraction so long as they are relevant, 24-year-old Bachelor's student Kirsten described how she appreciated the suggestions found in her Facebook feed:

> Eh, it's mostly concerts and eh.. clothing like fashion, ehm, and (pause) also a lot of university events and lectures and stuff like that, but a lot of it is something I search for myself, so it's obvious... but it's funny when you look at those ads, then you don't always think that this is because I searched for that or, like, you just think, 'wow, cool that they just find this for me' (laughs) or, like, totally naïve [...] I wouldn't think it's annoying that [ads] come up all the time, because I often think that they hit [the target] pretty well [Interviewer: And then it doesn't matter so much?] no, exactly, it's more if it's something that's not relevant at all or that you don't think is cool.

The responses falling under this theme are interesting because they often demonstrate somewhat advanced understanding of why relevant ads are being served in social media feeds, search results and so forth—that is, the respondents often approve of the systems enabling the relevance of the ads. In contrast, and distancing herself from her family, who also welcome ads in the form of physical magazines that arrive in the post every Saturday, Louise, a 30-year-old Master's student, explained how the actual relevance of online ads (unlike the physical ones her family reads through) is the exact thing that makes her want to escape them:

> I know what ads are and I get tempted by them, so I think it's nicer that it's just not there [...] sometimes [ads] even make me feel bad, thinking like... you've been looking at the same pair of boots for the seventh time and then you only get boot ads and then you just feel like, 'God my life is meaningless' (laughs).

'Free is a good price'

The fourth and last theme comprises responses that, more or less conscious of the underlying data business model, celebrate that because of tracking—and the targeted advertising, using profiling and so forth—these services are for free, at least in a monetary sense. Miriam, an airport employee, explained that it was exactly the fact there would be no monetary charge that intrigued her when she first started using social media:

> It's really good, the resources we have, and free on top of that, really good, but they should not control us, we should control them [...] I really got to use Facebook as part of establishing [a non-for-profit enterprise] eh, because I thought 'This is a free opportunity, there you have a free opportunity to reach a lot of people, but also a free opportunity to reach your family'.

Beyond the ease with which one can reach out, as articulated by Marie, a 36-year-old teacher, also emphasized another value in these services being free of monetary charge:

> I've heard some rumours saying that there's going to be payment on some of the different, I don't know if it's platforms or things you log into, and what's been positive until now is that if you have, if you can go online, then it's equal for all. Because you can visit the same pages irrespective of whether you're rich or poor and that's definitely a positive thing, but if you have to pay for it, then there's going to be a huge difference between who can afford this or that.

The quote by Marie celebrates the egalitarian principles that were foundational for the development of the world wide web, but it also demonstrates a lack of awareness about the price that is actually paid for free-to-download apps like the ones comprising our dataset. The fact that these services are not free in a literal sense, but only insofar as data rather than cash constitute the currency in which users pay for the services, does not figure anywhere as part of this understanding. Neither do circumstances surrounding inequality between people whose lives are heavily datafied and people whose lives are less tracked and shaped by data. Lastly, it disregards the imbalance between the commercial corporations harvesting and controlling people's data on the one hand, and individuals that are resigned to it as a result of successful corporate obfuscation on the other.

To sum up, the interview analysis confirms and elaborates on findings from previous user studies. The respondents express concern regarding online tracking while at the same time showing clear signs of resignation, as they lack the skills or knowledge to resist the datafication and surveillance of their everyday lives. The three themes of 'I have nothing to hide', 'As long as it's relevant', and 'Free is a good price' to some degree legitimize the tracking and commodification of users and indicate a normalization of the datafication mechanisms that are now heavily embedded in the respondents' everyday lives. 'It's scary', on the other hand, implies a more critical attitude, and suggests that the respondents would have an interest in countering datafication if they knew how to and

had sufficient knowledge on what is actually going on. The interviews thereby also point to the so-called trade-off fallacy: the prices and implications of using app-based communication services are blurred and opaque, thereby making it difficult to make informed decisions or rational cost-benefit-like calculations. As a result, in the respondents' accounts of how they experienced and understood online tracking, we found little or no information that could explain their experiences and understanding. Their accounts alone therefore proved to be insufficient for an analysis of the impact of mobile datafication. The following appscape analysis addresses head on the 'scariness' that the respondents expressed by exploring the direct and material consequences of their individual constellations of apps. By shedding light on the actual implications of mobile communication and making the underlying infrastructures visible, we hope to develop tools and resources that can show a way out of digital resignation and evoke active user engagement, empowerment and emancipation.

Appscape analysis

Building on the interview study above, the following analysis explores how datafication impacts the everyday lives of individual smartphone users from an infrastructural perspective. We first give an overview of the ten respondents, whose app repertoires we focus on for the analysis, and describe their apps, the number of permissions they request, and the third-party services they embed. We then zoom in on two respondents and compare their app repertories and the types of data harvesting and distribution enabled by them—that is, their appscapes. Lastly, we discuss how the appscape method can be a useful tool to enhance the transparency of app-based data collection and distribution and thereby increase the agency of individual users.

The respondents

Table 1 gives an overview of the ten respondents, their ages, occupations, total number of apps, total and average number of permissions requested by these apps, and the total and average number of third parties that the apps connect with.

While the 36-year-old teacher Marie has the highest number of apps (62), these apps, interestingly, require the lowest average number of permissions (15.4). At the other end of the scale, Ena, a 43-year-old day-care assistant, has just 11 apps, but these request an average of 29 permissions, which is the highest in the sample. Looking at the third-party services, Noah, a 21-year-old bar manager, has a total of 18 apps that connect, on average, to the highest number of third-party services (7.5). Also with 18 apps, the 30-year-old Master's student Louise connects to an average of just 3.9 third-parties. In order to understand these differences, it is necessary to take a closer look at the individual respondents' app repertoires. In the next section, we therefore identify the specific apps of two of the respondents, Noah and Ena, in order to explain their different constellations of permis-

Respondent	Age	Occupation	Apps total	Number of permissions	Ave. permissions	# of TPSs*	Ave. TPSs
Marie	36	Teacher	62	956	15.4	354	5.7
Kirsten	24	Bachelor's student	46	981	21.3	221	4.8
Fatma	25	Teacher	42	845	20.1	227	5.4
Stine	23	Bachelor's student	37	739	20	185	5
Louise	30	Master's student	22	581	26.4	86	3.9
Meriam	45	Airport staff	21	382	18.2	91	4.3
Noah	21	Bar manager	18	378	21	135	7.5
Sofia	28	Occupational therapist	16	408	25.5	66	4.1
Liam	52	Factory worker	16	350	21.9	69	4.3
Ena	43	Day care assistant	11	319	29	66	6

Table 1. Overview of respondents and their appscape data
**TPS = third-party service*

sions and third-parties. Noah and Ena are interesting and extreme cases (Yin, 2009) for a number of reasons, most notably that Ena's very limited app repertoire is particularly intrusive when it comes to accesses and permissions, and that Noah has a significant average third-party score for his apps.

App repertoires and permissions

With just 11 downloaded apps, Ena uses her smartphone for a more limited number of purposes compared to other respondents (e.g., Marie with 62 apps). The circular dendrogram in Figure 1 illustrates Ena's apps according to their category (the inner branches), the particular apps (the second-level branches), the accesses they request (the third-level branches), and the related permissions (the outer branches).

Three of Ena's apps are used for communication purposes (Messenger mainly for text messaging, Skype and Viber mainly for voice and video calls); three are categorized as social media (Facebook, Pinterest and YouTube); two are privacy protection apps (Adblocker and Adblock Plus); and the remaining three are respectively a game app (Bubble Witch), a finance app (MobilePay) and a weather app (TV2 Vejr). As the figure illustrates, the most invasive app in Ena's repertoire is Facebook, which requests a total of 52 permissions, including access to the calendar, camera, contacts, device and app history (allowing the app to access information on browsing history, for example), location, and so on. The communication app category, however, is the most invasive, requesting a total of 130 permissions across the three apps, with Facebook's Messenger app requesting 46 permissions alone.

In other words, Ena's preference for communication and social media apps is an important explanation as to why her average number of permissions is high. Interestingly, however, the two adblocker apps also account for a relatively high number of permissions

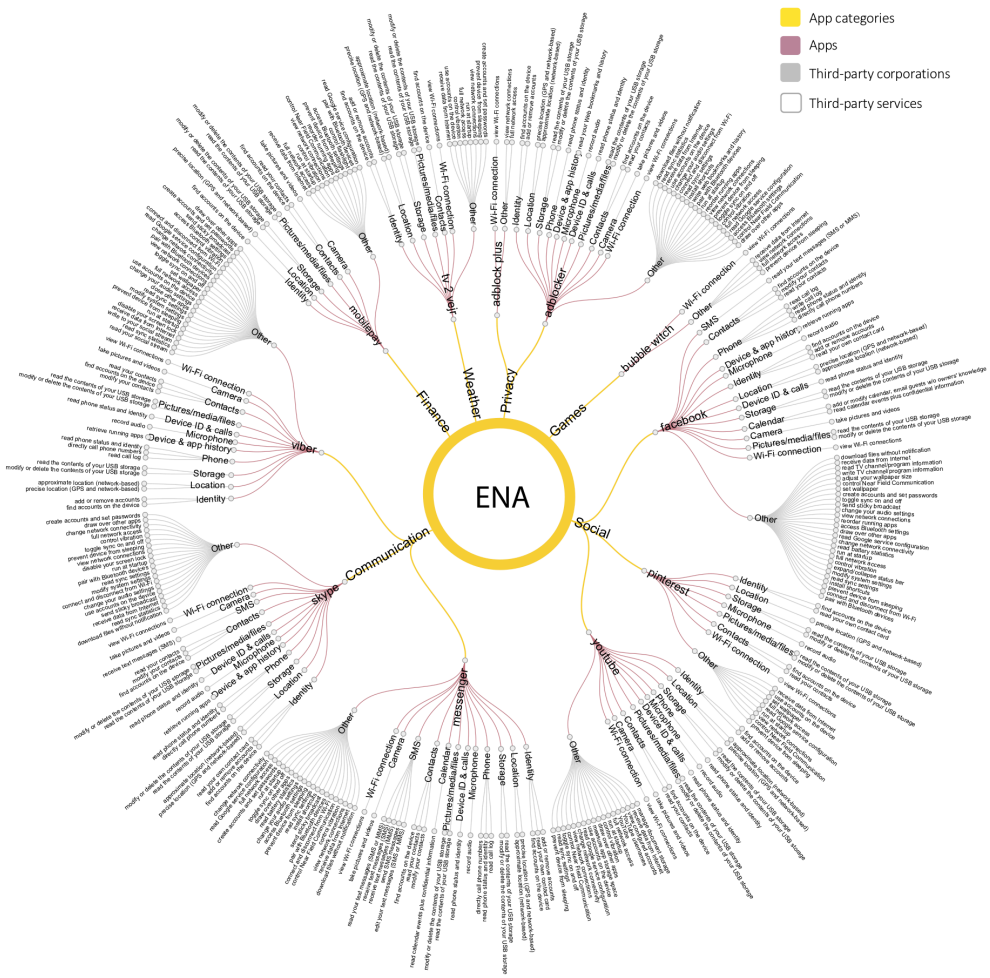

Figure 1: Ena's categories of apps, the apps, and their accesses and permissions.

(40 in total), but while Adblock Plus only requests three permissions, Adblocker request 37 permissions, including access to the phone's camera, contacts, device and app history, location, microphone and pictures. This is an interesting finding, as the two adblocker apps serve similar purposes but are remarkably different in terms of their degree of intrusiveness. Why does Adblocker need access to the camera, photos, calendar, browsing history and so on, if Adblock Plus does not? This question is difficult to answer without looking into the business models of the apps in question, but for the purposes of this article, we will simply note that the choice of a particular privacy tool is highly determinant of the level of intrusiveness to which a user is exposed. Put differently, increased awareness of the actual implications of choosing one app over another, as well as concrete tools to determine the differences between two seemingly similar apps, could lead to more informed user choices.

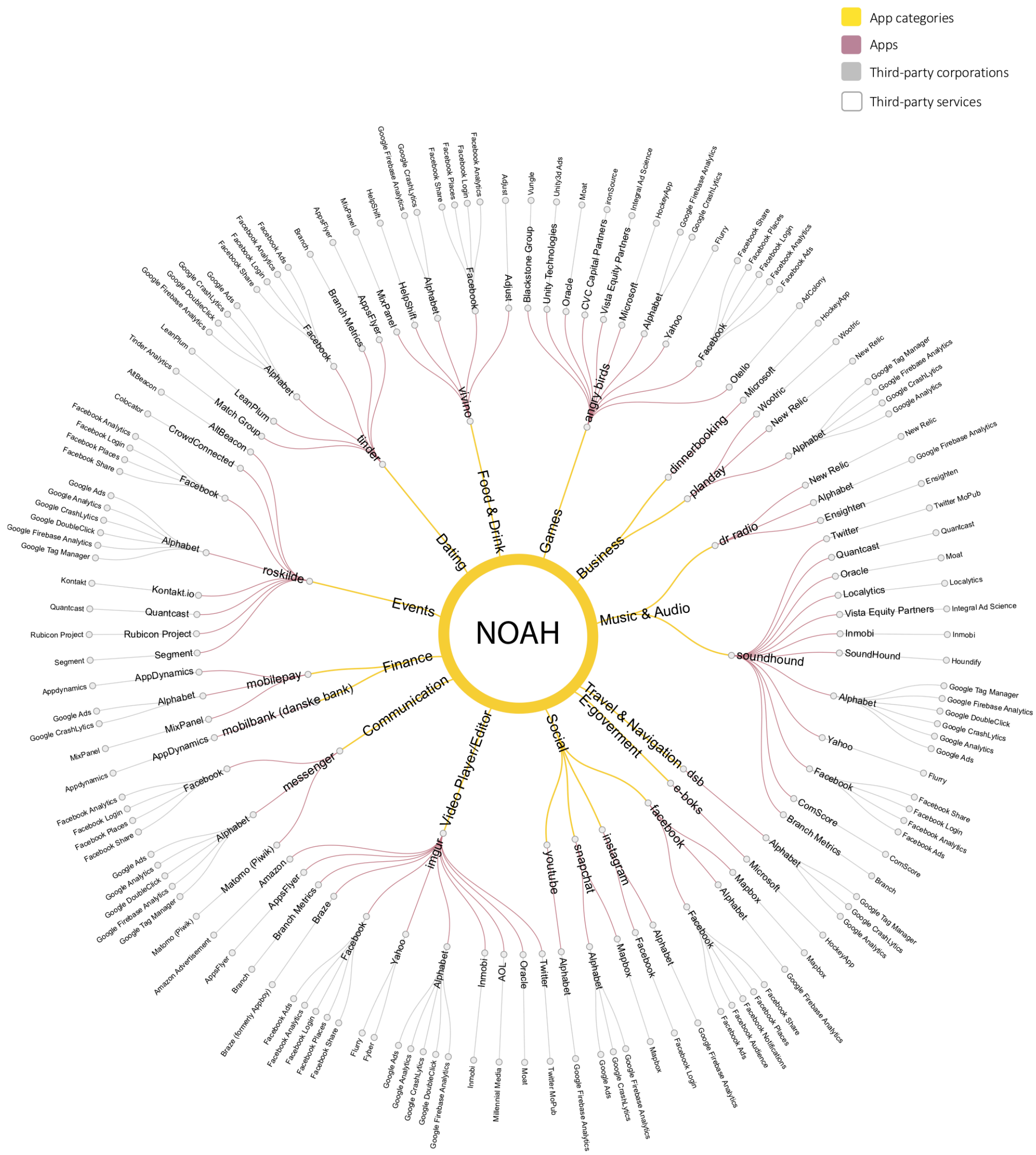

Figure 2: Noah's categories of apps, the apps, and their third-parties and third-party-services.

By strengthening transparency, users would be able to rise above the 'It's scary' attitude and challenge the 'Free is a good price' stance by being able to assess what kinds of data are paid in return for the service, and, importantly, existing alternatives. A closer look at the adblocker apps also reveals that Adblock Plus shares data with no third parties, while Adblocker connects to ten third-party services owned by, amongst others, Facebook and Alphabet. That is, Adblocker both collects a significant amount of meta data

and shares it with a relatively high number of third parties. The next section goes into depth on the impact and prevalence of third-party services, focusing on Noah's apps.

App repertoires and third-party connections

As listed in Table 1, Noah has downloaded 18 apps in total that connect to the highest average number of third-party services (7.5). Similar to Ena, the reason for the high number of third-parties is to be found in Noah's app repertoire, which is illustrated in Figure 2. Like in the figure above, the inner branches outline the categories of apps and the particular apps, while the two outer branches represent respectively the companies that own the third-party services and the particular third parties.

There is a clear overlap between the apps downloaded on Noah and Ena's phones. Noah also has the communication app Messenger and the social media apps Facebook and YouTube that, as described above, allow the collection of wide amounts of data. Apart from providing a significant degree of data to these apps, Noah's constellation of apps also allows a large number of third parties to access data. For instance, the music app SoundHound connects to 20 third-party services, the festival app Roskilde connects to a total of 16, and the dating app Tinder connects to 12. Across the apps, Alphabet and Facebook own more than half of the third-party services, but a long list of lesser known companies can also access Noah's data. These include, for instance, Leanplum and AppsFlyer that serve ads, and Tinder Analytics for performance monitoring and optimizing. While these apps share data with a significant number of third parties, they collect fewer data compared to Ena's apps. Tinder, for instance, asks for 18 different permissions, including access to the camera, location and pictures, most of which, at least to some extent, reflect the functionality of the app and the service provided (as Tinder allows you to upload and take pictures, search for potential partners nearby, etc.).

To sum up, Noah provides comparably fewer data to the specific apps, but (indirectly) allows the apps to distribute his data to a large number of market actors who utilize and monetize it in various ways (Joler & Petrovski, 2016). By uncovering this rather hidden ecology of apps and data, both users and scholars can be more informed when discussing and assessing data harvesting and reselling. Additionally, identifying the many actors involved in mobile surveillance can refocus attention away from the 'I have nothing to hide' position and towards questions of how and why apps and third parties collect data in the first place. This can, in turn, qualify knowledge building on how data are processed and returned to the user in more or less relevant, curated and filtered formats, providing a basis for the 'As long as it's relevant' attitude. In the following section, we will discuss how appscapes allow us to conceptualize, measure and compare the degrees of intrusiveness that different smartphone users are subjected to.

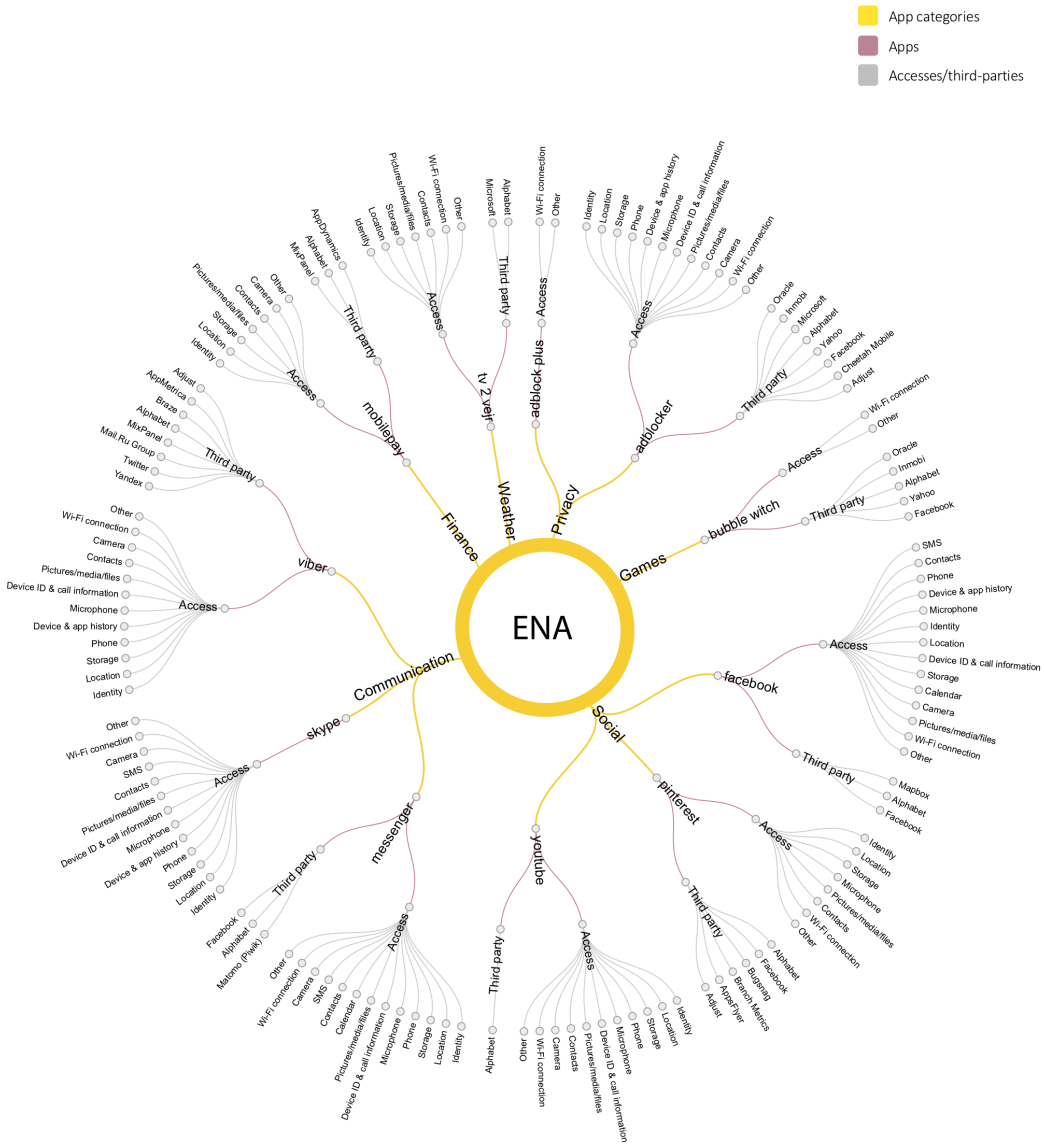

Figure 3: Ena's appscape. The visualisation overviews Ena's categories of apps, the apps, and the accesses they request on the phone as well as the third-party corporations, whose third-party services they embed. For overview purposes the permissions under each access are not featured, but can be found in figure 2 (for instance: the permissions to "add or modify calendar events and send email to guests without owners' knowledge" or the "read calendar events plus confidential information", which both reside under the access to "calendar"). The accesses alone relay information on the extent to which the app can harvest different types of data on the phone. Likewise, the figure does not include the specific third-party service under each third-party corporation (for instance: "Google DoubleClick" and "Google Tag Manager" are both owned by the Alphabet corporation). In other words, it show the number of potential actors that can access data irrespective of the number of third-party services they each embed in a given app.

Appscapes

Focusing on the app repertoires of Ena and Noah above, we have explored and explained their differences in terms of the number of permissions and third-party connections,

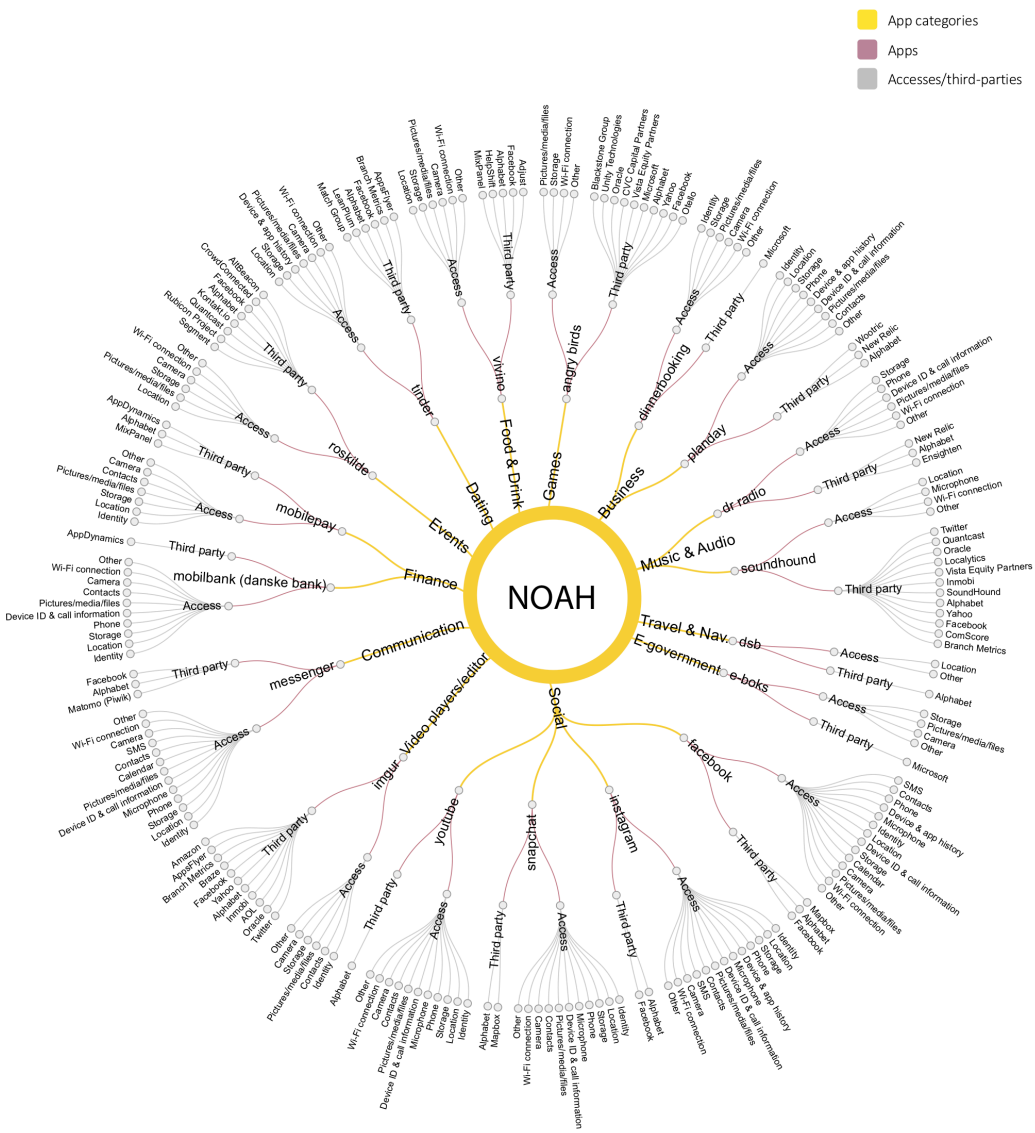

Figure 4: Noah's appscape. The visualisation overviews Ena's categories of apps, the apps, and the accesses they request on the phone as well as the third-party corporations, whose third-party services they embed. For overview purposes the permissions under each access are not featured, but can be found in figure 2 (for instance: the permissions to "add or modify calendar events and send email to guests without owners' knowledge" or the "read calendar events plus confidential information", which both reside under the access to "calendar"). The accesses alone relay information on the extent to which the app can harvest different types of data on the phone. Likewise, the figure does not include the specific third-party service under each third-party corporation (for instance: "Google DoubleClick" and "Google Tag Manager" are both owned by the Alphabet corporation). In other words, it show the number of potential actors that can access data irrespective of the number of third-party services they each embed in a given app.

listed in Table 1. The conceptualization of the appscape, as the specific constellation of apps, permissions and third-party connections pertaining to an empirical user, calculates the degree of intrusiveness. Figure 3 and Figure 4 illustrate Ena's and Noah's respec-

tive appscapes made up by the categories of apps installed on their phones (the inner branches), the permissions they request, and the third-party services they connect to (the two outer branches).

This approach allows us to measure and compare potential data disclosure on an individual level and visualize how data are harvested and distributed across the app ecology and data economy. It sheds light on datafication practices that are difficult to grasp for regular users, who then have a better foundation for choosing to interact with various types of mobile service. For instance, Figure 3 illustrates the kind of data Ena's apps collect and the third-parties that might harvest them. In other words, it provides valuable insight into meta data collection mechanisms and the ways data are transported, and raises important and critical questions for the data industry. The striking example of Ena's two adblocker apps, for instance, can operate as an eyeopener that allows users like Ena to make more informed choices in the common situation where several apps offer the same service. Furthermore, examples such as this can be an important step towards asking more critical questions of market actors and potentially increasing the efficiency and impact of regulatory initiatives.

Noah's appscape in Figure 4, similarly, testifies to the potential of the approach by illustrating how his every move—both on the smartphone and physically—can be tracked through the multitude of apps installed on his device. It also illustrates how the data can be distributed to known and less well known market actors that in various ways benefit from collecting and monetizing meta data. Finally, the appscape helps us connect the dots between the apps and the third-party services that are often owned by the same corporations—most prominently in our dataset, Alphabet and Facebook. In other words, the appscape method sheds light on the complex business models that finance what appear to be free services and thereby determine the conditions that regular users are forced to adhere to.

To sum up, the analysis compared ten different smartphone users' app repertoires and the ways data are collected and distributed though these services. By zooming in on two individual appscapes, we have investigated the implications of downloading different types of app, and visualized the data that are collected and the actors that access it, emphasizing how datafication and intrusiveness can be measured and monitored. In the final section, we discuss how the two analyses together inform the field of critical data studies by not only identifying the attitudes of regular smartphone users living out the datafication of everyday life, but also emphasizing how these attitudes are rooted in an infrastructural and commercialized environment characterized by opaque data collection, monetization and user commodification. Further development and implementation of the appscape approach in future research, along with consumer regulation, could be a step towards denaturalizing corporate obfuscation and empowering resigned users.

Implications and conclusions

This article has argued the need to combine user and infrastructure perspectives when studying the impact of datafication on smartphone users' everyday lives and thereby bridge the trenches that are so often dug between social constructivist studies of user understanding and materialist analyses of infrastructures. That is to say, datafication is both experienced by individual users and rooted in material infrastructures, and research should pay attention to both. By combining the human-centred focus of user studies with an infrastructural perspective that highlights material and economic macro-structures, our study enhances knowledge on how people's digital capabilities are framed by infrastructural conditions, and thereby how actual agency can be regained by building infrastructures for privacy.

In the interviews, the respondents demonstrated a variety of overlapping attitudes that all clustered around the feeling of digital resignation: data harvesting is understood as unavoidable and necessary, while at the same time being somewhat creepy, baffling and frustrating. The appscapes, in turn, map and provide evidence of the implications of particular app constellations and the ways in which tracking is enabled through mobile apps. They show that regular smartphone users, as represented by the respondents in the study, are heavily tracked through their smartphones. Taken together, the analyses show how the resignation that users express is embedded in the complex, obfuscated and inaccessible app infrastructure. Mobile datafication is, in turn, naturalized and expanded as a result of users' limited ability to critically interrogate and opt out of the conditions set up by powerful market actors that are in the business of trading in ever-increasing amounts of data. As argued by Draper and Turow (2019, p. 1833), "the corporate cultivation of digital resignation […] turns individual concerns about surveillance and privacy inward, leading individuals toward confusion and indecision (rather than toward collective action) about whether and how to take on the burdens of privacy self-management". This resigned, individualized and somewhat paralysed condition results in a lack of attention to and critique of "the broader surveillance ecosystems" and fails to facilitate "changes in industrial infrastructure that result in collective empowerment or systemic change" (ibid.).

We believe that the appscape approach paves the way for more effective solutions to counter digital resignation by fostering insights into the data harvesting and distribution systems that form the infrastructural foundation of individual smartphone users' everyday lives and the data economy alike. The appscape approach serves as an empirically grounded method to develop tools that allow both researchers and users to screen smartphones and apps and seek concrete guidance on how to choose between services and improve digital privacy—that is, without having to meticulously read through numerous pages of deliberately obfuscated terms of service agreements and privacy policies. We thereby join, and answer, Iliadis and Russo's (2016) call for critical data studies that "provide individuals with the necessary tools for becoming more informed and the ability to organize efforts around data justice issues" (p. 5). The prospects of the appscape

method, however, rest on the premise that increased awareness of datafication practices supports the existing informed consent processes and ultimately makes users more likely to resist or critically assess digital services. In effect, a critical next step for research is to engage with how people react to their individual appscapes. Only by confronting users—not only with the implications of their app usage, but also with suggestions for how to regain control of their data—will we be able to investigate the perseverance of phenomena such as the privacy paradox and digital resignation.

Acknowledgements

The research was partly funded by the Peoples' Internet project (the Carlsberg Foundation) and the Datafied Living project (the Independent Research Fund Denmark).

References

Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. *IEEE Security Privacy*, *3*(1), 26–33. https://doi.org/10.1109/MSP.2005.22

Atkinson, M., Olmstead, K., Smith, A., Hege, J., Heimlich, R., Amihere, D., Rubenstein, S., Greenwood, S., Rainee, L., Duggan, M., Porteus, M., & Paga, D. (2015, November 10). Apps permissions in the Google Play Store. *Pew Research Center: Internet, Science & Tech*. https://www.pewresearch.org/internet/2015/11/10/apps-permissions-in-the-google-play-store/, https://doi.org/10.2196/20009

Barth, S., & de Jong, M.D.T. (2017). The privacy paradox: Investigating discrepancies between expressed privacy concerns and actual online behavior: A systematic literature review. *Telematics and Informatics*, *34*(7), 1038–1058. https://doi.org/10.1016/j.tele.2017.04.013

Binns, R., Lyngs, U., Van Kleek, M., Zhao, J., Libert, T., & Shadbolt, N. (2018). Third party tracking in the mobile ecosystem. *Proceedings of the 10th ACM Conference on Web Science - WebSci '18*, 23–31. https://doi.org/10.1145/3201064.3201089

boyd, d., & Crawford, K. (2011, September 21). *Six provocations for big data*. https://papers.ssrn. com/abstract=1926431

Brinkmann, S., & Kvale, S. (2009). *Interviews, learning the craft of qualitative research interviewing* (2nd edition). California: SAGE Publications.

Bucher, T. (2017). The algorithmic imaginary: Exploring the ordinary affects of Facebook algorithms. *Information, Communication & Society*, *20*(1), 30–44. https://doi.org/10.1080/1369118X.2016.1154086

Cimpanu, C. (2019, September 11). Most Android flashlight apps request an absurd number of permissions. *ZDNet*. https://www.zdnet.com/article/most-android-flashlight-apps-request-an-absurd-number-of-permissions/

Couldry, N., & Yu, J. (2018). Deconstructing datafication's brave new world. *New Media & Society*, *20*(12), 4473–4491. https://doi.org/10.1177/1461444818775968

Dalton, C.M., & Thatcher, J. (2014, May). What does a critical data study look like, and why do we care? *Society+Space*, *3*(1), 1–9. https://www.societyandspace.org/articles/what-does-a-critical-data-studies-look-like-and-why-do-we-care, https://doi.org/10.1017/cbo9780511997389.005

Dencik, L., Hintz, A., Redden, J., & Treré, E. (2019). Exploring data justice: Conceptions, applications and directions. *Information, Communication & Society*, *22*(7), 873–881. https://doi.org/10.1080/1369118X.2019.1606268

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

Dubois, E., & Ford, H. (2015). Trace interviews: An actor-centered approach. *International Journal of Communication*, *9*(0), 25. http://ijoc.org/index.php/ijoc/article/view/3378

Ellison, G., & Ellison, S.F. (2009). Search, obfuscation, and price elasticities on the internet. *Econometrica*, *77*(2), 427–452. https://doi.org/10.3982/ECTA5708

Exodus. (n.d.). *Exodus privacy*. Retrieved from https://reports.exodus-privacy.eu.org/en/

Falahrastegar, M., Haddadi, H., Uhlig, S., & Mortier, R. (2014). The rise of panopticons: Examining region-specific third-party web tracking. In A. Dainotti, A. Mahanti, & S. Uhlig (Eds.), *6th International Workshop, TMA 2014* (pp. 104–114). Springer. https://doi.org/10.1007/978-3-642-54999-1_9

Galloway, A.R. (2004). *Protocol: How control exists after decentralization*. MIT Press.

Iliadis, A., & Russo, F. (2016). Critical data studies: An introduction. *Big Data & Society*, *3*(2), 1-7. https://doi.org/10.1177/2053951716674238

Jensen, K.B. (2013). Definitive and sensitizing conceptualizations of mediatization. *Communication Theory*, *23*(3), 203–222. https://doi.org/10.1111/comt.12014

Joinson, A. N., Reips, U.-D., Buchanan, T., & Schofield, C.B.P. (2010). Privacy, trust, and self-disclosure online. *Human–Computer Interaction*, *25*(1), 1–24. https://doi.org/10.1080/ 07370020903586662

Joler, V., & Petrovski, A. (2016, August 21). Immaterial labour and data harvesting. *Share Lab*. https://labs.rs/en/facebook-algorithmic-factory-immaterial-labour-and-data-harvesting/

Kalavri, V., Blackburn, J., Varvello, M., & Papagiannaki, K. (2016). Like a pack of wolves: Community structure of web trackers. In T. Karagiannis, & X. Dimitropoulos (Eds.), *Passive and active measurement. Lecture notes in computer science*, vol. 9631 (pp. 42–54). Springer. https://doi.org/10.1007/978-3-319-30505-9_4

Kennedy, H., & Hill, R.L. (2017). The feeling of numbers: Emotions in everyday engagements with data and their visualisation. *Sociology*. https://doi.org/10. 1177/0038038516674675

King, N., & Horrocks, C. (2010). *Interviews in qualitative research*. London: SAGE.

Kitchin, R. (2013). Big data and human geography: Opportunities, challenges and risks. *Dialogues in Human Geography* 3(3), 262-267. http://journals.sagepub.com/doi/10.1177/2043820613513388

Kitchin, R., & Lauriault, T.P. (2018). Toward critical data studies: Charting and unpacking data assemblages and their work. In J. Thatcher, J. Eckert, & A. Shears (Eds.), *Thinking big data in geography* (1st ed., pp. 3–20). Lincoln, Nebraska: University of Nebraska Press. https://doi.org/10.2307/j.ctt21h4z6m.6

Lai, S.S., & Flensburg, S. (2020). A proxy for privacy uncovering the surveillance ecology of mobile apps. *Big Data & Society*. http://journals.sagepub.com/doi/10.1177/2053951720942543

Lai, S.S., Pagh, J., & Zeng, F.H. (2019). Tracing communicative patterns. *Nordicom Review*, *40*(s1). https://doi.org/10.2478/nor-2019-0019

Light, B., Burgess, J., & Duguay, S. (2018). The walkthrough method: An approach to the study of apps. *New Media & Society, 20(3)*, 881–900. https://doi.org/10.1177/1461444816675438

Marcus, G.E. (1995). Ethnography in/of the world system: The emergence of multi-sited ethnography. *Annual Review of Anthropology*, *24*(1), 95–117. http://www.annualreviews.org/doi/abs/10.1146/annurev.an.24.100195.000523

Mayer-Schönberger, V., & Cukier, K. (2013). *Big data: A revolution that will transform how we live, work, and think*. Boston, MA: Houghton Mifflin Harcourt. https://doi.org/10.3359/oz1314047

Musiani, F., Cogburn, D., Denardis, L., & Levinson, N. (Eds.). (2016). *Turn to infrastructure in internet governance*. Springer Nature. http://link.springer.com/openurl?genre=book&isbn=978-1-349-57846-7, https://doi.org/10.1057/9781137483591

Nieborg, D.B., & Helmond, A. (2018). The political economy of Facebook's platformization in the mobile ecosystem: Facebook Messenger as a platform instance. *Media, Culture & Society*, *41*(2), 196–218. https://doi.org/10.1177/0163443718818384

Norberg, P.A., Horne, D.R., & Horne, D.A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, *41*(1), 100–126. https://doi.org/10.1111/j.1745-6606.2006.00070.x

Oomen, I., & Leenes, R. (2008). Privacy risk perceptions and privacy protection strategies. In E. de Leeuw, S. Fischer-Hübner, J. Tseng, & J. Borking (Eds.), *Policies and research in identity management* (pp. 121–138). Springer US. https://doi.org/10.1007/978-0-387-77996-6_10

Patton, M.Q. (2015). *Qualitative research & evaluation methods: Integrating theory and practice* (4th edition). Thousand Oaks, California: SAGE Publications, Inc.

Pötzsch, S. (2009). Privacy awareness: A means to solve the privacy paradox? In V. Matyáš, S. Fischer-Hübner, D. Cvrček, & P. Švenda (Eds.), *The future of identity in the information society* (pp. 226–236). Springer. https://doi.org/10.1007/978-3-642-03315-5_17

Sandvig, C. (2013). The internet as infrastructure. In W. H. Dutton (Ed.), *The Oxford handbook of internet studies*. Oxford: Oxford University Press. https://doi.org/10.1093/oxfordhb/9780199589074.013.0005

Vallina-Rodriguez, N., Sundaresan, S., Razaghpanah, A., Nithyanand, R., Allman, M., Kreibich, C., & Gill, P. (2016). Tracking the trackers: Towards understanding the mobile advertising and tracking ecosystem. *ArXiv:1609.07190 [Cs]*. http://arxiv.org/abs/1609.07190, https://doi.org/10.14722/ndss.2018.23353

Weltevrede, E., & Jansen, F. (2019). Infrastructures of intimate data: Mapping the inbound and outbound data flows of dating apps. *Computational Culture*, *7*. http://computationalculture.net/infrastructures-of-intimate-data-mapping-the-inbound-and-outbound-data-flows-of-dating-apps/

Winseck, D. (2019). Internet infrastructure and the persistent myth of U.S. hegemony. In B. Haggart, K. Henne, & N. Tusikov (Eds.), *Information, technology and control in a changing world* (pp. 93–120). Springer International Publishing. https://doi.org/10.1007/978-3-030-14540-8_5

Yin, R. K. (2009). *Case study research: Design and methods*. Thousand Oaks, California: SAGE Publications, Inc.

Young, A.L., & Quan-Haase, A. (2013). Privacy protection strategies on Facebook. *Information, Communication & 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* (1st edition). New York: PublicAffairs. https://doi.org/10.4000/qds.3723

Signe Sophus Lai
Department of Communication
University of Copenhagen

Sofie Flensburg
Department of Communication
University of Copenhagen