Low on trust, high on use datafied media, trust and everyday life

Mathieu, David; Hartley, Jannie Møller

Original Research Article

Low on trust, high on use datafied media, trust and everyday life

David Mathieu[1] (iD) and Jannie Hartley-Møller[1] (iD)

Abstract

This article explores yet another paradox – aside from the privacy paradox – related to the datafication of media: citizens trust least the media they use most It investigates the role that daily life plays in shaping the trust that citizens place in datafied media. The study reveals five sets of heuristics guiding the trust assessments of citizens: (1) characteristics of media organisations, (2) old media standards, (3) context of use and purpose, (4) experiences of datafication and (5) understandings of datafication. The article discusses the use of these heuristics and the value that everyday life holds in assessing trust in datafied media. It concludes that, guided by a partial 'structure of perception' and enticed into trusting datafied media in the context of their daily lives, citizens may be highly concerned by the datafication of media but use them nevertheless.

Keywords

Trust, datafied media, everyday life, datafication, media use

Introduction

On 19 February 2020, the European Commission for a Europe Fit for the Digital Age unveiled its strategy concerning data and artificial intelligence. One of the cornerstones of this vision is the idea of 'trustworthy technology',[1] with the aim that Europe becomes a 'trusted digital leader'.[2] The executive vice president of the commission, Margrethe Vestager posited in a speech on 29 October 2020: 'and the more we come to understand how much we depend on these platforms – and how little we really understand or control the choices they make – the more people's trust in digital technology begins to waver. And without that trust, we won't be able to get the most out of the potential of digitisation'.[3]

The normative importance of trust expressed by Vestager refers to a functional definition of trust (Frederiksen, 2017) that underlines the role that trust plays for the good functioning of society and the cooperation between citizens and institutions. Media such as Facebook or Google, which massively collect data from citizens, are arguably becoming the Achile's heel of this functional trust (Zuboff, 2020). More and more, citizens are invited to question the trust they give to datafied media. And as these media are highly integrated in citizens' everyday life, they likely have a strong influence on the perceptions that citizens entertain towards the datafication of

society. This article explores in an empirical study how Danish citizens negotiate their trust to datafied media in the context of their everyday lives. By datafied media we mean the platforms, websites and apps that collect, store, analyse and retroact user data to optimise and personalise user experience, for example in the form of recomender systems of predictive analysis (Mathieu and Pruulmann Vengerfeldt, 2020).

The article begins by developing the theoretical framework linking together trust, datafied media and everyday life. It then presents the methodology for this research, the focus group interview. The analysis is divided into two sections. The first analytical section examines everyday life as a site of encounters with datafied media and identifies five sets of heuristics – or everyday logics – that citizens use to assess trust. The second part of the analysis discusses the role that everyday life plays in the assessment of trust. The article concludes that everyday life provides an environment in which citizens are enticed to make trust in datafied media work out.

[1]Roskilde University, Roskilde, Denmark

Corresponding author:
David Mathieu, Roskilde University, Roskilde, Denmark.
Email: mathieu@ruc.dk

Trust, everyday life and datafied media

Scholarship on trust shows that everyday life provides an ontological source of trust. The phenomenological tradition regards trust as an ontological reality (Giddens, 1991: p. 129) that is based on the 'non-calculative form of familiarity' (Frederiksen, 2017: p. 2) provided in our everyday lives. We have a natural tendency to trust in the world we know, to trust that things are fine, and that they will continue to be in the future. As Giddens (1991) puts it: 'people's assumption of normalcy and familiarity in their dealings with social and natural worlds serves as a 'mantle of trust' that 'brackets risk' (quoted in Frederiksen, 2017: p. 4).

Everyday life has been conceptualised as a site of struggle against the system (De Certeau, 1984; Lefebvre, 2014). But it is also a site of resolution of the conflicts that arise between the lifeworld and the system. Not only is everyday life a site of resistance and rebellion, but citizens also wish to resolve these conflicts so that life can go on, resuming its ordinariness and sense of balance.

> Our everyday lives are the expression, in their taken-for-grantedness, as well as their self-consciousness, of our capacity to hold a line against the generalised anxiety and the threat of chaos that is a sine qua non of social life. In this sense everyday life is a continuous achievement more or less ritualised, more or less taken for granted, more or less fragile, in the face of the unknown, the unexpected or the catastrophic. (Silverstone, 1994: p. 165).

Pink et al. (2018) show how everyday life provides a structure of familiarity that helps resolve data anxieties. They develop the concept of 'data anxiety' and the related concept of 'everyday trust' to demonstrate how everyday, improvisatory actions enable citizens to feel comfortable despite the messiness of datafication. They investigate everyday life circumstances as emergent, attending to how people improvise to fill in the gaps between what they think they know about data and the inevitable uncertainties that their actions entail. In these everyday life contexts, the practices of citizens are 'idiosyncratic and improvisatory' (Pink et al., 2018: p. 2).

Similarly, we are concerned with how citizens render data acceptable and comfortable, but, departing from the work of Pink et al., we are concerned with datafication as more than the storage of important and private information and the risk of their loss. For us, experiences of datafication result from use, and hence, we relate datafication to the use of media, adopting an audience approach in analysing how citizens make sense of and develop trust in the datafied media they use in their everyday life.

Everyday life and the familiarity that citizens have towards media may provide an aura of trust, but citizens are also asked to relate to the datafication of media, something they are less familiar with and which is often characterised in the literature as being opaque, hidden and invisible. In that context, and given the contradictory forces at play between familiarity and strangeness, how do citizens evaluate, negotiate and make sense of their trust in datafied media?

We posit that everyday life provides a 'structure of perception' (Schutz, 1970) with which to comprehend and make sense of datafied media. That is, we conceive everyday life as an environment that provides diverse occasions to become familiar with datafied media and their risks and benefits. These encounters provide a subjective basis from which citizens evaluate their trust in datafied media. This phenomenological perspective on datafication is acknowledged in various studies on the public perception and public understanding of data and algorithms (Lomborg and Kapsch, 2019; Lupton and Michael, 2017; Michael and Lupton, 2016; Ytre-Arne and Moe, 2020).

Trust as situated in datafied media

Ostherr et al. (2017) have studied the 'evolving concept of trust' in the context of health, in particular the differences between the context of medical research and self-monitoring practices. They argue that trust is more easily given in the context of social media, apps and 'user-generated culture' than in research protocols. This finding suggests that trust is embedded in cultural and everyday contexts that affect how citizen see and give their trust In other words, trust is not an individual or rational decision provided in a vacuum, but is situated in a web of concrete meanings and practices.

An interesting but often overlooked aspect of trust revealed by that study is that this assessment is made *in context*. Modern media have been part of citizens life for more than a century and form an important part of our socialisation and identity at all stages of life. We therefore need to understand how trust in data is given by citizens in the context of media use, as the two aspects are conflated in everyday life, which is what this article sets out to do.

A consideration for the context of media use has influenced the methodological path taken by this study and has allowed to uncover an interesting paradox in our data: Citizens trust the least the media they use the most. The paradox is interesting because it challenges our expectations about rational response. A rational approach would argue that if citizens were concerned by datafied media, they would limit their use of media.

This finding can be compared with the privacy paradox (Barth and de Jong, 2017), which shows that, despite being concerned with their privacy, citizens do little to protect themselves about privacy breaches and risks. Draper and Turow (2019) explain that users resign themselves to have their privacy invaded as they are left with the prospect

of opting out of media in the face of their concerns. Our study goes further, however, in that it problematises the relation between trust and media use. In doing so, this article contributes to the conversation about trust in datafication by looking specifically at the context of media consumption.

While a lot has been said on the collection of personal data, and the privacy issues it brings, we regard the datafication of media as a more encompassing tendency that includes aspects of data infrastructure (Arsenault, 2017), data analysis, data-driven governance, on top of the collection of a wide range of data.

Data collection by the media, whether legacy or social media platforms, is nothing new; media organisations have in the past and still do collect demographic or psychographic data on their audience without giving rise to major concerns. However, the scale and intensity at which data is now collected, analysed and acted upon, as revealed in scandals such as Cambridge Analytica (Hu, 2020), are alarming the public. Digital media, their website, platforms and applications, have become a major purveyor of citizen data. The omnipresence of digital platforms, forming a substantial part of today's media ecosystem, makes data extraction ubiquitous and applied to a wide variety of human experiences.

Not only has data changed in scope but also in nature, as media are extracting data in the form of post-demographics (Rogers, 2015) such as likes, shares and comments, meta-data such as location or time (McCosker, 2017) and inferred data in the form of profiles (Cheney-Lippold, 2017), on top of personal data made available by users. Many argue that these data are facilitating the commodification and manipulation of media audiences (Turow, 2011), encroaching their privacy (Draper and Turow, 2019), but also their integrity (Zuboff, 2020) and their identity (Cheney-Lippold, 2017).

Data was arguably not something that citizens were encouraged to worry about in the context of legacy media. But as digital media made data extraction, analysis and governance extensive, systematic and ubiquitous, the public has been invited by whistleblowers, journalists, scholars, policy makers and politicians to worry about data. This is a new reality for citizens, who now need to evaluate how their use and reliance on media is to be weighted against the risks associated with datafication.

An audience sense-making approach

The theoretical framework of this study is anchored in an approach that sees audience agency, sense-making and everyday life as central to our understanding of media consumption. Audience research is an approach that looks into how media consumption, and any effects that follow, is situated in the everyday life of media users. According to Sonia Livingstone (2007), such an audience approach needs to take into considerations the three following aspects:

1. The context of everyday life as a site of appropriation of media;
2. Audience literacy, that is, what audiences know and how they actively use their knowledge and experiences to make sense of their media consumption;
3. Power relations between media and audiences, and especially the agency that audiences possess in order to respond to media power.

Applying an audience research means understanding media consumption as a site of negotiation between media power and everyday life. This notion of negotiation is important as media effects are not conceived as direct and linear, but always mediated by the interpretative resources and contexts that are brought to bear on media consumption. By extension, we contend that the negotiation of trust is shaped by the conditions and constrained provided by media, but also by the experiences and resources brought by socially situated audiences. In consequence, the theoretical framework of audience helps understand trust, not as an individual decision given in a vacuum, but as a highly contextual and situated phenomenon.

Thus, we understand the assessment of trust in datafied media to be mediated by these three aspects of media consumption. Accordingly, our study has been guided by these three questions:

- How does everyday life and everyday use of media contextualise the negotiation of trust?
- What knowledge do audiences draw upon to negotiate trust in datafied media?
- What agency are audiences given by media to negotiate their assessment of trust?

Methodology

The focus group method was used to explore how everyday life mediates the trust of citizens in datafied media. We interviewed 34 participants from the municipality of Roskilde, Denmark. The municipality, situated 30 kilometres from the Danish capital Copenhagen, was chosen because it comprises both urban and rural areas. Participants were recruited both randomly, contacted on open streets and shops around town and from there the sample was expanded through the so-called snowball method. The participants were divided into four groups based on age (18–35 vs. 35–60) and education (short vs. long[4]) and took place from December 2018 to February 2019. Groups were kept homogenous in terms of age and level of education in order to facilitate discussions (Bloor et al., 2012; Halkier, 2008). The distribution of participants into different groups was done to achieve maximum variation (Halkier, 2008) in order to uncover different ways by which trust interfaces with everyday life. Comparative analyses between the four different groups were not attempted;

instead, these groups were used as contexts for interpreting interview statements taken to be expressions of the structural categories (age and education) which these groups reflect. Each focus group was conducted by two researchers (one moderating and one taking notes), audio-recorded and transcribed according to basic conventions. Written consent of research participants was obtained prior to the focus groups, interview statements were anonymised and audio recordings were erased following their transcription.

The focus group discussions were organised in three phases. In the first phase, participants were invited to name the media they used regularly and which they believed to collect and use their data. A broad range of legacy and new media along with platforms and technologies that are not usually considered media, were mentioned, attesting of a blur between media and technologies amongst our participants. The first phase provided an icebreaker as well as a way to scope the research. The second phase asked participants to rank the media previously mentioned on a trust scale (see Illustration 1). The objective was not to measure trust but to stimulate discussions and allow participants to articulate the reasons behind their choices. In the third phase, we confronted participants with different messages regarding data collection that they were likely to have encountered, such as GDPR reconsent campaign e-mails, cookie declarations or data policies. The objective of this phase was to explore the awareness of citizens and the coping mechanisms they use to deal with datafied media.
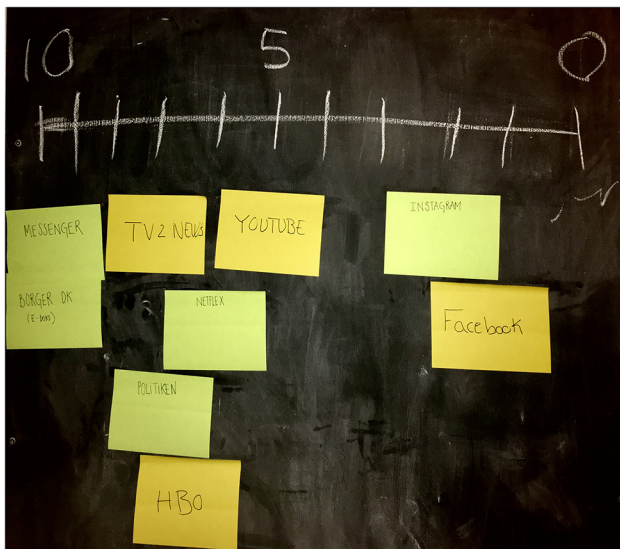

Illustration 1: the placement of media on the trust scale in one focus group (From left: high trust, to right: low trust).

The data were coded in two rounds. In the first round, the notions of everyday life, literacy and agency were used as sensitizing concepts to explore the data and uncover the emic perspective of citizens. The goal was not to impose rigid codes to the data for the purpose of standardization

and structuration needed for statistical analysis. Rather, the coding was realized as a way to explore patterns in the data. Overall, we paid attention to the diverse ways everyday life provided occasions for citizens to trust or mistrust datafied media: the context in which trust assessments occur, whether trust responses are accompanied by agency or literacy, and what understandings of risks and data are involved. Once an analytical focus was identified, which we based on the notion of heuristics (see next section), a more systematic coding was undertaken to cover all possible meanings mentioned by participants.

Focus groups are no replacement for direct observations or other behavioural measures. However, such studies would be difficult to set up, and the ability to observe would be limited in a study on trust in the context of everyday life. Focus groups were chosen to allow participants to freely draw on episodes, practices and routines that they find meaningful, uncovering, in a relatively short time, a very broad range of responses within a variety of everyday contexts with a diversity of media.

Hence, focus groups do not allow a measurement of the trust that citizens have in datafied media, but they provide valid data on the ways in which people think about it. We did not define 'trust' or 'datafied media' prior to the study but allowed participants to speak freely about what these topics meant for them in the context of their everyday lives. As such, interview statements are important for the categories of meaning and the 'cultural distinctions' that they reveal, rather than for providing a truthful representation of a reality outside the interview situation (Alasuutari, 1995).

Everyday heuristics of trust in datafied media

Everyday life provides contexts for encountering, evaluating and making sense of data and risks. Through these encounters, citizens use heuristics to assess their trust in datafied media. 'Judgment heuristics' are everyday logics that provide shortcuts used for decision making, replacing more extensive, deliberative and rational reasoning used to draw conclusions (Fischhoff, 2001). In the context of trust, these heuristics serve to inform citizens on the likelihood that certain media present trust issues. These heuristics reflect the subjective experience of citizens based on their encounters with data. It is not surprising that citizens rely on heuristics to establish their trust in datafied media, given the limited technical knowledge that is publicly available on data collection and analysis.

The focus group discussions led to the identification of around 30 different criteria by which citizens make sense of datafied media. These criteria can be further divided into five main categories: (1) characteristics of media organisations, (2) old media standards, (3) context of use and purpose, (4) experiences of datafication and (5) understandings of datafication. These heuristics are reproduced in

Typology of heuristics to assess trust in datafied media
← Less trust   More trust →

1) Characteristics of media institutions

Privately owned	versus	Publicly owned
Commercial *	versus	Non-Commercial
Not regulated	versus	Regulated
Free to use	versus	Paid
New	versus	Established
Monopolistic	versus	
Bad brand	versus	Good brand
Small (security)	versus	Big* (security)
Big (more invasive)	versus	Small* (less invasive)
Foreign	versus	National

2) Old media standards

Entertainement	versus	News
More time spent	versus	Less time spent
Poor quality of content	versus	High quality of content
Presence of ads	versus	Absence of ads

3) Context of use and purpose

	versus	Commercial*
Frivolous	versus	Important/serious/useful
Open purpose	versus	Well-defined purpose
Purpose incoherent w/ data	versus	Purpose coherent w/ data
Public*	versus	Private
SoMe	versus	All other media

4) Experiences of datafication

Complicated/Opaque	versus	Clear
Obvious misuse	versus	Ethical
Unknown	versus	Known
Constrained / forced	versus	Freely given / Collaborative
Less control	versus	More control
Automatic	versus	Require consent
Extensive and varied	versus	Restricted

5) Understandings of datafication

Involvment of personal data	versus	Absence of personal data
Login or account	versus	No loggin or account
More connectivity	versus	Less connectivity
Intense surveillance	versus	Little surveillance
Sensitive personal data	versus	Non-sensitive personal data
Sell my data	versus	does not sell my data

Figure 1. Typology of heuristics used to assess trust in datafied media.

Figure 1 in the ways they have been expressed during ordinary conversations in the focus groups. As such, some heuristics may appear redundant and repetitive, while some may be said to be implied by others, but we found it important to rely on the words of participants in describing their subjective experiences.

These heuristics appear in the form of semiotic oppositions (such as 'black' being defined as the opposite of 'white' and vice-versa) rather than through stable, intrinsic characteristics. Semiotic meaning can be unstable as it varies with time and context depending on the oppositions to which it is associated. Furthermore, citizens draw simultaneously on different heuristics when evaluating their trust in datafied media. The meaning and importance of these heuristics vary depending on context. The same heuristic can, in one context, influence trust positively, while do so negatively in a different context (these are marked with an asterisk in Figure 1). Some heuristics may even cancel each other out.

In the citation below, a participant assesses the SoundCloud platform, which he contrasts with Spotify. The citation provides an example of the complexity involved in assessing trust, as different heuristics are identified. It also illustrates the semiotic oppositions involved in this rationalisation:

> Well, I'm thinking in relation to Spotify … I'm thinking that maybe [SoundCloud] is not as business-like. Also because there is no advertisement, and it's free to use. It's easy to open an account if you want access to their functions, but it's voluntary. And it's made for artists who are more underground and who want to be known. So I'm thinking that it's … I don't have any problem with that platform (younger group with longer education).

In this evaluation, many heuristics leaning towards trust are used: SoundCloud is not a big (invasive) company. It does not present advertisements. While an account can be opened, which is usually understood as a means of data collection and hence, not trustworthy, the participant stresses that this account is optional in order to use the platform. Media that are free to use are usually understood as being strongly motivated to monetise data collection. But this aspect of SoundCloud is presented as positive in the citation, possibly because there is no requirement to identify oneself to be able to use the platform (which is of course a misconception if the platform uses cookies or other tracking devices). SoundCloud is also said to have a good brand serving artists and the underground community. All these contrast with the characteristics of Spotify, which is mainstream, big and invasive, requires an account to use, serves ads, in which free is clearly associated with audience commodification.

Characteristics of media organisations

These heuristics have little to do with datafication but consider media as institutions. They are heuristics that could be used in all sorts of encounters and not just those regarding datafication. In that sense, they are criteria about general aspects of institutional trust, and one could say that datafied media are 'borrowing their reputation' from the general trust in these institutions. In these cases, trust in datafied media is given by association due to considerations other than datafication.

One of the main heuristics that characterises the trust of Danish citizens in datafied media is the distinction between public and private institutions. In general, Danes have a high level of trust in their public institutions compared to citizens of other nations in Europe and the rest of the world (OECD, 2013). This trust in public institutions is therefore borrowed by media that are state-owned or that assume public functions, such as the public service broadcaster, Danmarks Radio (DR), or the many digital platforms providing services to citizens which Danes have become acquainted with in the past decade.

> I think [I have more trust] because it's the state that acts as the sender. One way or another, it could well be that they collect our data for this or that reason, but I assume that there is no unethical purpose behind it. Plus, they have all my personal information in the first place, so I'm thinking: What is it they want to know more about me? How often I use the service? I don't mind them knowing that (older group with longer education).

In a similar vein, national institutions inspire more trust than foreign ones, which in practice often refer to American or Chinese media:

> Also with TV2 [(a subscription-based TV network)], I think it matters that we take it to be Danish. I think we have a tendency to consider that some things that are very Americanised … or what comes from China … there are many hackers and what not, you know. So you feel safer for some reasons (younger group with longer education).

With this main heuristic comes a host of similar distinctions that are used to emphasise different aspects of the private versus public dialectic. Public institutions are usually more strictly regulated, which is a source of trust With the advent of the GDPR, however, private and commercial institutions are seen as becoming more regulated and hence, can be trusted: 'I expect that they can deliver. I mean, that we can all have trust that they live up to the rules that exist in relation to data protection, that they do what they can against data leaks. Don't you think?' (younger group with longer education).

The heuristic 'commercial' carries a very specific meaning for citizens. When a platform is deemed 'commercial', its main goal is to make money, and that is a reason to be wary of its datafication practices, as citizens are well aware that their data has commercial value (although they have difficulties understanding the nature of this value). Our participants are not naïve regarding the commercial intentions of media and digital platforms, including platforms provided by non-media organisations such as banks: 'Well, a bank is also a business. Of course they have to sell some products; they have to keep the mill running. So it is clearly a business' (older group with longer education).

Hence, a commercial organisation, such as Facebook, is more likely to engage in dubious or extensive datafication practices. Similarly, paid services, such as Netflix or HBO, are better trusted than free services, as data collection is a known way to monetise a free service, again with Facebook serving as a prime example. Being an established or a new institution, in the particular contexts in which this was discussed, refers essentially to a distinction between pre-Internet legacy media versus media that are native to Internet. The participants have more trust in news organisations that predate the Internet than in those that have established themselves since the advent of Internet. Facebook is seen to be in a monopoly, dominating social media, almost too big an organisation, which in the mind of citizens, means more invasive. However, being a big tech company also has an advantage when it comes to issues of safety, as big companies are seen as more reliable and more competent on the technical aspects of storage and security than small companies: 'Some of these apps, they are so big; we should feel safe using them. For example, Facebook' (younger group with shorter education). In this respect, public companies are seen to be at a disadvantage, and even a big institution such as the Danish state is seen as lagging behind giants such as Facebook and Google.

The large size of an organisation can be positive or negative. It is seen as positive with regards to the competences that a company is assumed to have in order to secure its data but is a threat because, according to one participant, it is easier to hide data practices:

> Talking of big companies, then of course they have a lot of security, but they can also take data from a single person without people realising it. Let us say that they had three persons in there, and they suddenly took data from a person, then people would take notice. Whereas, when there are millions of people, then they can hide it more easily (younger group with shorter education).

Having a good brand or a particular image that attracts confidence inspires more trust. This is the case of the Reddit platform, which, to users, is community-based and anarchist, values that are in opposition to datafication, the system.

In contrast, and unsurprisingly, Facebook has received a bad image in the press over the past few years, and this is reflected in its brand. Although Facebook is not well trusted, our participants find it difficult to identify the exact problems plaguing Facebook.

Old media standards

The heuristics from this category are similar to those from the category above; however, they pertain specifically to legacy media and the standards relating to these media. In other words, these heuristics predate Internet media but are applicable to them. The standards that these legacy media have established in the minds of their audiences are transferred to datafied media in order to assess their trust, and yet these criteria have nothing to do with datafication. Datafied media are then judged using the standards that individuals hold for legacy media.

It is well known in audience research that media audiences associate the consumption of news with social desirability, while the consumption of entertainment is viewed negatively. Hence, entertainment media are seen as less trustworthy compared to news media. Spending a lot of time watching entertainment is regarded pejoratively, and this bias is evidenced in expressions such as 'heavy viewers' of television or so-called 'couch potatoes', who are seen as more vulnerable and less resourceful than other viewers. The risk attached to the notional 'heavy viewer' is acknowledged by a participant: 'It is because you use it a lot that you become nervous and you have less trust. Because it becomes riskier the more you use it' (younger group with longer education).

The quality of the content is a determinant of trust, and clickbait content damages such trust. An important heuristic that comes up repeatedly in our discussions with participants is the presence of ads. If a media publishes ads, it is immediately seen as a commercial organisation, which is understood as a strong incentive for collecting data. The presence of ads provides one of those strong signals that alarms citizens, and the phenomenon of creepiness is no stranger to that, as revealed in this quote:

> It's not meant for Facebook to know about this. If you, for example, search for a driving licence some place [online], then it starts to come up from three different places. It's a bit like, ads are showing up in places you don't really want them to (younger group with shorter education)

Contexts of use and purpose

Compared to the two previous categories, the remaining three categories of heuristics are more directly concerned with datafication. The third category, the context of use,

is rather important for citizens, because it is associated with different risks.

The commercial heuristic comes up again, but this time, it is seen as a sign of trust. This is because the commercial nature of a media organisation clarifies what citizens can expect in terms of data practices, and individuals can therefore act accordingly to protect themselves: 'they play with open cards because they are a business' (younger group with longer education). One group of young participants with short education discussed at length how they restrict what they reveal publicly on commercial platforms in order to avoid having their data misused. One citizen explains how, in that respect, Google should be considered: 'I think it concerns the idea that Google makes me a product, and they try to make ads targeted at me. And I feel that it's something you should know when you open a Google account' (younger group with longer education).

Another distinction that cuts across the entertainment versus news heuristic is whether the media serves a frivolous or a serious, important or useful purpose. Participants attribute more trust to LinkedIn than any other social media platform because of the seriousness of its purpose. They trust to a lesser degree the media whose purposes are varied, such as Facebook, than those with well-defined purposes, such as Instagram (although the two platforms belong to the same company). This also explains why media that provide services to citizens are well trusted: the collection and use of data serves a clear purpose, an aspect that will be revisited in the next category of heuristics.

> I think it depends [on] what you use it for. I don't use www.borger.dk [a hub for governmental services to citizens] very much, but I use it for an important purpose. The same with my netbank. Well, I use it every day, but I use it for an important purpose. All the crap that's actually just 'bla bla bla, click here, read that', I use it quite a lot, but it's superficial. When you sit on the toilet and get bored … It's stuff that doesn't mean anything to me, but I can end up spending quite a lot of time on it (older group with longer education).

Citizens are also aware if the data collected and stored on a platform is related to the purpose of the service delivered. The website www.borger.dk collects personal information about citizens in order to securely identify them and provide needed services, and this is well understood by citizens. However, explaining why Snapchat stores individuals' pictures on its servers is more difficult for the participants. An effective heuristic related to this discussion is classifying media into social, versus other types of media. All social media are ranked lower on trust Although they are not always given the same rank, using social media always rings the alarm bell of mistrust.

Finally, a heuristic that proves very important for many participants in the focus group is the distinction between a private context of use, in which the audience is more restricted and recognizable, such as Messenger or Snapchat, and a public context of use, in which the audience is larger, if not potentially infinite, such as Facebook, Instagram or LinkedIn. Our participants consider public contexts much riskier, but this risk relates exclusively to a conception of data as personal data, either in the form of content that is uploaded on a media platform or sensitive information such as location or telephone number. Participants fear that personal data can be misused by malevolent people, such as hackers, identity thieves or sexual predators, more so than by the platforms.

Experiences of datafication

This category concerns the way citizens encounter datafication in their everyday life. These encounters point towards the importance of the visibility of datafication in everyday life. Many participants discuss episodes that have 'opened their eyes', such as when a participant googled himself: 'I happened to Google myself once and found out that, even though I have a private profile, some of my pictures are in fact accessible. It consternated me' (younger group with longer education).

When the context of datafication is opaque, complicated, unknown or obviously prone to abuse, citizens have unsurprisingly less trust in these media. The definition of abuse, however, varies a lot, and the threshold is not necessarily very high: the creepy nature of advertisements and situations in which datafied experiences of using media are retroacted unwillingly to audiences are seen as abusive.

> 'Creepiness' (Lupton and Michael, 2017; Ruckenstein and Granroth, 2019) is one of the main ways in which citizens think about trust issues. Individuals are for example concerned, when their searches and clicks on the web are being translated into advertisements on connected platforms, such as Facebook. Creepiness presents itself as a general phenomenon in the minds of the participants in this study, and also occurs when synchronising a newly bought phone, receiving unsolicited notifications from Google about traffic conditions, etc. Participants find many aspects of datafication to be creepy.

When citizens have no or little control over the data given, when they are forced to provide data or when data collection takes place automatically, trust suffers. It is worth noting that participants do not consider their consent to terms of service as a form of everyday consent for these practices to legitimately take place. When using services such as Google, users necessarily have to accept the terms of services, effectively giving their consent to Google to use their data how Google deems fit. However, in everyday

life, when the datafication of their experiences of using media creeps up unexpectedly, participants are rather baffled: 'I think it's odd because it's like they stalk me, and I don't think I have said yes to that' (older group with longer education). Participants also react to what they perceive as extensive datafication. In that respect, 'Google is scarier than Facebook' (older group with shorter education).

Being forced to provide data, especially in the context of entertainment, for example, having to provide an e-mail address to be able to take a quiz, is seen as very suspicious. Netbanks, most of which are associated to a physical bank, profit from the face-to-face relationships that they have established with their clients. Participants trust the data collected by netbanks, because of the relationship established with their bank advisor, but also assured that they will be compensated if something goes wrong (as banks are regulated):

> The reason I'm comfortable with netbanks, for me it's related to our bank, to the dialogue we have around taking a loan, child saving, etc. There is a trust relation that is established with your banker or with the netbank, and I trust them with my data. But it's done within the framework of a relationship to which I have agreed (older group with longer education).

Platforms such as ForældreIntra, Aula or Family (digital communication platforms between schools and parents) have pervaded the Danish school system over the past decade and are usually regarded with suspicion in terms of the risks they involve. One parent, generally quite concerned with datafication, discusses how she trusts the platform used at her kid's school. She explains how the school called a meeting with the parents to discuss how the platform is used, what data is collected and why and how it complies with the GDPR. Based on collaborative personal and human relationships, the parent's concerns are met, and trust is established. Such a cooperative approach is in stark contrast to the ways by which media platforms usually ask citizens for consent and trust, which are impersonal, automatic and oftentimes implicit.

Understandings of datafication

Individuals encounter datafication through direct contact with the media, but their understanding of datafication is also shaped by their interpersonal relationships. Having a parent or significant other that has professional knowledge on datafication promotes awareness, and incidentally, mistrust, as can be seen in this quote: 'I don't trust them, but it's mostly because my dad works in IT. So he knows, like, where you need to look and those kinds of things' (younger group with shorter education).

The construction of datafication by citizens is highly discursive, and various practices contribute to a mistrust in datafied media. Aside from social relations, participants learn about datafication through the media. They hear about it in the news and other informational programmes, which have been a major source of mistrust:

> *I think Facebook, Instagram and Messenger are less trustworthy than Netflix. [Interviewer: Why is that?] Because there has been so much talk about all this data craziness* (younger group with shorter education).

> *Him, from So Ein Ding* [a technology TV programme on the Danish public service television]. *Do you know him from TV? He goes a lot into it, all things technology, and he knows a lot about it … and you know, the world is going down (…)* (older group with longer education).

The involvement of personal data, such as credit card numbers, is understood as a factor of risk (it is sometimes, but not always, a factor of trust[5]). In some focus group discussions, it is seen as the main or sole risk for certain citizens. Thus, media platforms that require personal information or that require users to log in or have memberships are viewed with suspicion. Participants often understand that these are 'mouse traps' to obtain data, more so in contexts of entertainment or when the purpose for data collection appears unclear. For example, one participant differentiates between two ways of obtaining data:

> *(…) But there is no need to login. It's a bit the same with what was said previously about 9gag* [a social media platform based in Hong Kong]. *That if you only go there without opening an account, it could well be that they track my IP-address, at least to see that I come from Denmark, but I think it's fine (younger group with longer education).*

Another aspect of datafication that bothers participants concerns the connectivity between media or services, the idea that data travels from one media platform to another or what participants refer to as 'talking together' (younger group with longer education) or, even more problematic, the idea that data are being sold. They regard these practices negatively, even if it takes place within the same company, such as the connectivity that may exist between Facebook and Messenger.

We can see, in such examples, how trust emerges from the use of these media platforms. These heuristics, namely the involvement of personal data, login, connectivity and the selling of data, do not represent a technical understanding of what goes on behind the scenes or within the black box of datafied media but rather, represent the possible risks that follow from specific uses of datafied media.

The extent of surveillance is also an area of concern, but surveillance was not a dominant topic of conversation amongst our participants. One participant, however, distinguished between different media platforms in terms of surveillance: 'I'm thinking that you are not being watched the same way [on Netflix than] on Facebook' (older group with longer education). The distinction is probably related to the kind of data that is collected on each platform. Netflix is paid, private and has a useful algorithmic personalisation feature, while Facebook is free, involves a public context, involves ads, etc. While Netflix may appear more trustworthy than Facebook, in effect, it has similar opportunities to monitor user data and exploit it (see Matthew, 2020).

The type of personal data provided is also important. As an example, one participant is more concerned by having her pictures collected than her e-mail collected:

> *I think pictures have more weight than e-mails. Pictures of me. Personal messages have more weight than, what is it called … the Internet … that I have been to see TV2 News* [a television news channel also accessible from the Internet] *or what else. This way … but I don't know. There could be ways by which they can use this information that I don't know about … So it's like, I'm in the dark* (younger group with longer education).

Indeed, this participant does not suspect that her e-mail address is much more valuable to marketers than her picture, as the former can be used to link her with other kinds of data collected about her. Here, the personal, e.g. pictures or messages, is seen as the most sensitive kind of data, regardless of how other kinds of data are used.

The role of everyday life in the trust of datafied media

The objective of this section is to discuss everyday life as a context for providing trust in datafied media. We are especially interested in understanding what agency is provided to citizens and how it is constrained or shaped by everyday life. We argue that everyday life provides a 'structure of perception' (Schutz, 1970) that is at best incomplete and partial for the purpose of assessing trust in datafied media. Furthermore, as trust is assessed in the context of media use, the latter provides a counter-weight to trust issues, offering a power of attraction so strong that it detracts citizens from engaging fully with the trust issues they identify.

It is interesting to reflect on the space that Facebook occupies in the minds of the participants. It is as though the sum of heuristics reported applies specifically to reflect the mistrust engendered by Facebook. 31 out of the 32 heuristics that lean towards mistrust can be said to apply to Facebook. As such, Facebook represents the token of mistrusted datafied media, and indeed this media came up frequently as a topic in the discussions we had with citizens. By contrast, DR, the public service media, represents a token of trust for Danish citizens. It is an organisation that Danes have known well over many years and which carries out a legitimate public role.

With the notion of token, we wish to emphasise that citizens understanding of trust is not abstract, but concrete and strongly anchored in their experience of media. Facebook, for instance, is a token of mistrust in datafied media because it channels all there is to say about mistrust. Talking about mistrust in datafied media and talking about Facebook are thus essentially the same.

In between the two poles that Facebook and DR represent, different media seem to instanciate different trust assemblages. Netflix and HBO are talked about mostly in relation to algorithmic personalisation, which is seen by young participants as useful (whereas the same logic did not apply to Facebook). Digital platforms, such as Mobile Pay (a mobile payment application) or www.sundhed.dk (the official internet-based portal for the public healthcare system), are mostly understood in terms of the purposes they serve and users' experiences of datafication. Interestingly, although Messenger belongs to Facebook, it is evaluated differently because of the private context of use it affords. All these media are seen as more trustworthy because they are thought in terms of specific features of datafied media that are not regarded as risky, veiling from consciousness other aspects that would be considered problematic.

That is, citizens experience datafied media in terms of token representing specific types of trust assemblages. For Schutz (1970), these frames of reference allow individuals to navigate their everyday life experience, but we see these trust assemblages to be possibly misleading for several reasons. First, they do not always represent the objective conditions known about datafication. Second, they present many contradictions or inaccuracies that bias the assessment of trust. Third, they form a basis of knowledge that effectively limits the assessment of trust that can be made.

DR is no doubt engaged in data practices. It was however shocking, for many of our participants, to learn that DR let Facebook and Google collect cookies and track users within its platform. The reputational capital acquired over the years may have provided the broadcaster an aura of trust which obscured its engagement in datafication.

There are several other examples in which one could doubt that the everyday heuristics identified by citizens provides an objective basis for evaluating data practices in the media. Our respondents differentiate between public and private media, social media and non-social media, news and entertainment, etc., but it can be argued that all these media engage in rather similar data practices. For citizens,

the presence of ads signals mistrust, yet non-commercial organisations also engage in datafication and practices that are considered problematic, such as the automated decision-making (Kaun and Velkova, 2019).

Many participants posit that logging into a service will result in more data collection or that uploading content on social media platforms accounts for most of the risks related to datafication. While not untrue, these statements are only part of the reality of datafication and hence, basing judgment on them may provide a false sense of security. Similarly, the many reconsent e-mails that individuals have received in the wake of the GDPR were understood as an indication that companies were not handling data properly, which is not necessarily the case.

A salient example for how these assemblages limit the assessment of trust concerns the conception of data and risks typical of especially the young users of Facebook. Concerned with issues of self-presentation, these young people understand data as personal information, ignoring concepts such as behavioural data (clicks, etc.), metadata or inferred profiled data. They understand risk primarily as the misuse of personal information. The surveillance, manipulation or exploitation associated with data collection do not enter their preoccupation, and cookie declarations appear to them mostly as a source of distraction and irritation. They regard behavioural data as harmless ('of course they are allowed to know what I see on TV'), irrelevant outside the context of everyday life ('they can't really threaten me with the movies that I see') or not serious ('It's not serious [data]. Indeed, there is nothing personal there').

It is interesting to see how different, contradicting logics are entertained by our respondents. Not considering oneself to be at risk and yet expressing mistrust in datafied media. Such an apparent contradiction is quintessential to everyday life and says a lot about the effort invested by citizens to make things work. The assessment of trust in datafied media made by citizens does not escape this kind of everyday logic. Consider this quote:

> Yes, well, I'm not much concerned by that because you can just avoid putting sensitive information that can be harvested. I have more trust towards Instagram because they don't take so much information compared to Facebook (younger group with shorter education).

On one hand, this participant admits to not being bothered by the risk of datafied media, and yet, establishes a distinction of trust between two different media platforms (which, ironically, belong to the same company). The young participants especially, take it upon themselves to minimise the risks associated with their use of datafied media. Mistrust may arise, but it is resolved by controlling the kind of personal data shared on media or the security settings of the platform. It is precisely by taking action against a mistrust in datafied media that trust is materialised. Such trust is not invested in the media, however, but in one's ability to minimise risks. As one participant puts it: 'it's my job not to give them too much' (older group with longer education).

The individual responsibilisation expressed in the quote above is a consequence of making datafied media work in everyday life, which relieves media of their responsibility to engage in appropriate and ethical data practices. While this shows that citizens are not passive towards datafication, it also means that they accept the normalcy of the issues it raises:

> Well, of course you have [a] responsibility to take care of your data. For example, you can decide to leave your phone number on Facebook, or you can decide if you wish your location to appear on Snapchat. So you can't expect Facebook and Snapchat not to … If you share this info yourself, then you can't expect that there won't be anybody to use it (younger group with shorter education).

As citizens wish to move as smoothly as possible in the realm of their everyday life, mistrusting datafied media inevitably results in small, if not complete, interruption of the flow of their everyday life. For example, we can see how mistrust is discouraged by the dependence of modern social relations to media platforms:

> My daughter goes to dance lessons and they communicate on Facebook. I am not on Facebook myself, and I certainly don't want my kids to be on Facebook. But if she has to be a part of it, she is forced to use it (older group with longer education).

If citizens were to join thought with action, their mistrust would lead them to avoid media altogether. As datafied media is so embedded in the conduct of everyday life, a complete distrust in datafied media – what is called for by the likes of Zuboff (2020) – is very hard to live up to because it would demand a complete reorganisation of the role of media in everyday life as we know it today.

Conclusion

Citizens can be said to hold a complex and multi-faceted understanding of trust in datafied media. They assess their trust in relation to how they see media organisations, to standards established by legacy media, to the purpose and use of data collection, to how they experience datafication and to understandings of datafication made available to them. The fact that we found such varied and sophisticated means of assessing trust indicates that citizens are concerned with the datafication of media. We can also conclude that citizens express mistrust in datafied media, but that this mistrust is essentially a discursive construction; one that does not match with their practice of using media.

While everyday life provides a source of concern for citizens in their dealings with datafied media, it is also a site of resolution of these concerns and conflicts. Datafication first appears to be disruptive of the relationship between citizens and media, aptly expressed in their discursive mistrust. Citizens are then left with the task of resolving these disruptions as best they can, which allows them to come to terms with that aspect of their everyday life. Trusting datafied media in that context is not an endorsement of the data practices of media.

As everyday life provides a limited structure of perception and a context in which media occupy a dominant place, it leaves a vast margin of manoeuvre for media to engage in unethical and problematic data practices before citizens can envisage to pull the plug. Also, given the tendency of citizens to make things work in the context of their everyday life, we cannot expect the public to be the only barometer of these data practices, least the catharcis for change. In that sense, citizens are given a burden that is unfair and difficult to fulfill given how trust in datafied media is situated in their everyday life. The tendency to sometimes blame or make citizens responsible for the management of their privacy seems unfair, as they are simply responding to the conditions that are made available to them and trying to make the system work in the context of their daily lives. Rather, we need to recognise how trust is situated in the context of media use.

While data literacy to some extent represents a promising path for enhancing the structure of perception of citizens, we see several canveas that need to be addressed before doing so. Bringing more awareness to data practices, asking for more transparency or providing more knowledge to citizens, might not necessarily lead to literacy. We can see in our focus group discussions how knowledge and awareness lead not to literacy, but to more worries, showing how the issue is also emotional and not simply cognitive. Surely, there are also limits to what we can ask citizens to know in order to be able to take stance towards datafied media.

In practice, new knowledge is integrated into everyday structures of perception, but as we have showed, as long as these structures are skewed towards media use, the role that literacy can play is limited. Because trust is situated in media use, citizens weight risks associated to datafied media against the many ways these media are anchored and support their everyday life. Furthermore, we also noted how opportunities for literacy interrupt the normal flow of everyday life and are seen as distraction and nuisance by some citizens. It could be argued that citizens are simply not interested to be confronted with knowlegde of datafication, as it would make their use of datafied media, which they depend on in their everyday lives, a worrying practice.

On a more positive note, the negotiation of trust in everyday life, and the paradox it exposes, could be taken as an indication that citizens do not completely reject the datafication of media. While inadequate, the heuristics presented in this study say something about the standards and preferences by which citizens would like to engage with datafied media. Citizens appreciate serious and purposeful use of data, but are against the commodification of their experience and identity in the context of entertainment. They are bothered by the creepiness that results from hidden or unwilling datafication. They contend that datafication should take place in the context of an explicit, consensual and substantial relationship, rather than something done behind their back. Data practices should be developed in familiar contexts by trusted actors for clear purposes, braced by regulation, instead of serving unknown or dubious purposes, developed as commercial experiments in a data Farwest. Until these standards are respected, citizens may be reluctant to fully invest their trust in datafied media.

ORCID iDs

David Mathieu https://orcid.org/0000-0003-1317-5056
Jannie Hartley-Møller https://orcid.org/0000-0001-5784-2864

Notes

1. https://ec.europa.eu/commission/presscorner/detail/en/ip_20_273
2. https://ec.europa.eu/commission/presscorner/detail/en/ip_20_273
3. https://ec.europa.eu/commission/commissioners/2019-2024/vestager/announcements/speech-executive-vice-president-margrethe-vestager-building-trust-technology_en
4. Typically, those with 'short education' have spent a maximum of 13 years in the Danish system (primary school followed by short trade, business or high school), while the category "long education" includes those who have spent between 14 and 21 years in the Danish system (high school plus university or similar long specialized education). Very few people over 18 in Denmark have less that 13 years of education. Source: https://akkr.dk/akkreditering/videregaende-uddannelser/

5. 'I have in fact confidence in them because it's linked with my bank card, and I'm not overly concerned that it can be misused' (older group with longer education).

References

Alasuutari P (1995) *Researching Culture: Qualitative Method and Cultural Studies*. London: Sage Publications.

Arsenault AH (2017) The datafication of media: Big data and the media industries. *International Journal of Media & Cultural Politics* 13(1): 7–24.

Barth S and de Jong MDT (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.

Bloor M, et al. (2012) *Focus Groups in Social Research*. London: Sage Publications.

Cheney-Lippold J (2017) *We Are Data: Algorithms and the Making of Our Digital Selves*. New York, NY: NYU Press.

De Certeau M (1984) *The Practice of Everyday Life*. Berkeley: Univ. of California Press.

Draper NA and Turow J (2019) The corporate cultivation of digital resignation. *New Media & Society* 21(8): 1824–1839.

Fischhoff B (2001) Judgment heuristics. In: Wilson RA and Keil FC (eds) *The MIT Encyclopedia of the Cognitive Sciences*. Cambridge: The MIT Press, pp. 423–425.

Frederiksen M (2017) Trust In: Turner BS (ed.) *The Wiley-Blackwell Encyclopedia of Social Theory*. John Wiley & Sons, pp. 1–9. Available at: https://onlinelibrary.wiley.com/doi/book/10.1002/9781118430873 (accessed 14 December 2020).

Giddens A (1991) *Modernity and Self-Identity: Self and Society in the Late Modern Age*. Stanford, CA: Stanford University Press.

Halkier B (2008) *Fokusgrupper*. Frederiksberg: Samfundslitteratur.

Hu M (2020) Cambridge analytica's black box. *Big Data & Society*, 7(2): 1–6.

Kaun A and Velkova J (2019) Automated decision making in Sweden. In: Spielkamp M (ed.) *Automating Society. Taking Stock of Automated Decision-Making in the EU*. Germany: AW AlgorithmWatch gGmbH, pp. 126–131.

Lefebvre H (2014) *Critique of Everyday Life: The One-Volume Edition*. London: Verso.

Livingstone S (2007) The challenge of engaging youth online: Contrasting producers' and teenagers' interpretations of websites. *European Journal of Communication* 22(2): 165–184.

Lomborg S and Kapsch PH (2019) Decoding algorithms. *Media, Culture & Society* 42(5): 745–761.

Lupton D and Michael M (2017) 'Depends on who's got the data': Public understandings of personal digital dataveillance. *Surveillance & Society* 15(2): 254–268.

Mathieu D and Pruulmann Vengerfeldt P (2020) The data loop of media and audience. *MedieKultur: Journal of Media and Communication Research* 36(69): 116–138.

Matthew JR (2020) Netflix and the design of the audience. *MedieKultur: Journal of Media and Communication Research* 36(69): 52–70.

McCosker A (2017) Data literacies for the postdemographic social media self. *First Monday* 22(10).

Michael M and Lupton D (2016) Toward a manifesto for the 'public understanding of big data'. *Public Understanding of Science* 25(1): 104–116.

OECD (2013) *Trust in Government, Policy Effectiveness and the Governance Agenda*. Paris: OECD Publishing.

Ostherr K, et al. (2017) Trust and privacy in the context of user-generated health data. *Big Data & Society* 4(1): 1–11.

Pink S, Lanzeni D and Horst H (2018). Data anxieties: Finding trust in everyday digital mess. *Big Data & Society*, 5(1): 1–14.

Rogers R (2015) *Digital Methods*. Cambridge: The MIT Press.

Ruckenstein M and Granroth J (2019) Algorithms, advertising and the intimacy of surveillance. *Journal of Cultural Economy* 13(1): 12–24.

Schutz A (1970) *Reflections on the Problem of Relevance*. New Haven: Yale University Press.

Silverstone R (1994) *Television and Everyday Life*. London: Routledge.

Turow J (2011) *The Daily You: How the New Advertising Industry is Defining Your Identity and Your Worth*. New Haven: Yale Univ. Press.

Ytre-Arne B and Moe H (2020) Folk theories of algorithms: Understanding digital irritation. *Media, Culture & Society* 43(5): 807–824.

Zuboff S (2020) *The Age of Surveillance Capitalism: The Fight For a Human Future at the New Frontier of Power*. London: Profile Books.