Human Soheil and Cech Florian

A Human-centric Perspective on Digital Consenting: The Case of GAFAM

Conference or Workshop Item (Accepted for Publication)
(Refereed)

A Human-centric Perspective on Digital Consenting: The Case of GAFAM

Soheil Human and Florian Cech

1 Introduction

According to the European General Data Protection Regulation (GDPR) "[t]he protection of [all] natural persons in relation to the processing of personal data is a fundamental right" (GDPR 2016, Recital 1) [20, Rec. 1]. The concept of end-user given consent plays an important role in digital regulations such as the GDPR. As a result of its enforcement and other legal obligations, data controllers have widely developed consent-obtaining mechanisms in recent years. Although consent is *only one of the possible bases* for lawful practice of data processing based on the GDPR (see [20, Article 6]), obtaining consent is still widely practiced and it can be perceived as an important means, which can potentially enable an end-users' *agency* regarding the management and ownership of their personal data.

While the GDPR expects specific prerequisites for a lawful consent, which should be *valid*, *freely given*, *specific*, *informed* and *active*, it is clear that this requires *consent-giving agents*, i.e. the end-users, to be able to provide and *manage* such consents [31]. Previous research, however, shows that the majority of people do not seem to be empowered to practice their digital right to privacy and lawful *consenting*. As an example, a European Commission's Special Eurobarometer with the title "Data Protection" [16], which was conducted in 28 EU member states with nearly 28.000 participants, sheds some light on how people deal with their digital privacy. Most end-users do not seem to have the necessary legal and technological information required to actively protect their personal data [16]. Only 20% of

Soheil Human
Sustainable Computing Lab & Institute for Information Systems and New Media, Vienna University of Economics and Business (WU Wien), Austria.
e-mail: soheil.human@wu.ac.at

Florian Cech
Centre for Informatics and Society, Vienna University of Technology (TU Wien), Austria.
e-mail: florian.cech@tuwien.ac.at

respondents to the European Commission's survey have said that they are always informed about the conditions and further uses of data collection. 41% of the respondents said they are only sometimes informed. 22% have said that they are rarely informed about these issues, and around 11% replied that they are never informed. On the topic of legal authorities, 37% said that they knew about their national authority for data protection, whilst 61% said they did not. Furthermore, reading privacy policies and terms of use before starting to use a service is time consuming. When asked how much control they feel they have over the information they provide online, 15% of participants said they have complete control, 50% said they have partial control and 31% said they feel no control at all. In an environment where users are connected to many digital technologies, keeping track of every privacy policy involved becomes an impossible task. Therefore, many users are unwilling and poorly equipped to deal with the numerous privacy policies they face with. In the aforementioned Eurobarometer, participants were asked about the reasons why they do not fully read privacy policies and 67% of them found policies too long to read while 38% responded that the policies were unclear or difficult to understand [16].

Considering the disappointing results of the Eurobarometer and the vast amount of other research endeavours with similar implications [46, 47, 50, 52], we propose that end-users need to be empowered in terms of their right to *consent* (including their right to withdraw their consents at any time) by interdisciplinary and mutli-dimensional socio-technical means and approaches. Based on the *enactivist* [26, 32, 51] perspective in cognitive science, in this paper, we propose a basic human-centric framework for end-user empowerment wherein *consenting* is considered a *sociocognitive action* which includes *cognitive*, *collective*, and *contextual* dimensions. We subsequently apply this framework to evaluate the practice of consent-obtaining by the 5 biggest tech companies, i.e. Google, Amazon, Facebook, Apple, Microsoft, whose consent-obtaining mechanisms affect lives of billions of humans around the globe. After presenting our evaluation methodology and results, which show that these companies do not follow a human-centric approach towards obtaining end-users' consents, we provide a concise discussion on the research presented and outline future work.

2 The Need for a Human-centric Perspective on Digital Consenting

While research shows that many of the people who are involved in online activities are aware that their personal data is being collected and shared, this gives no concrete proof to assume that people are willing to give away their personal data [44]. On the contrary, the importance of digital privacy to people has been demonstrated. People even "develop innovative strategies to achieve privacy while participating in the systems that allow them to access information, socialize with

friends, and interact with contemporary entertainment platforms"[44] (see also [11, 12, 42, 43]).

A similar line of thought is expressed by Busch [13] as well, who emphasizes that whilst people's professed interests in maintaining privacy do not always line up with their actual behavior, we might want to consider that a) individual choices are not fully rational and b) small decisions of individuals accumulate into large consequences that all users (i.e. all humans) have to face. On this matter, as [4, p. 27] reminds us: "the question whether do consumers care?" is a different question from "does privacy matter?". We affirm both of these questions. However, we believe that answering a third question is even more important: *if most of the end-users do care about their privacy and if privacy does matter, how can people be empowered to really practice (enact) their privacy-values?* If we accept that "the individual end-users and their needs and values, as well as the environment (including socioeconomical contexts, other actors, etc) and technologies they interact with, continuously co-create the [...] end-user empowerment" [29] (see also [6, 30]), only an approach which considers all these different involved dimensions can truly enable human empowerment. We call such an approach *human-centric*, wherein individual (cognitive) and social (collective & contextual) dimensions of every single end-user and all end-users combined are taken into account when an information system–a consent-obtaining mechanism in our case–is designed, implemented, evaluated, and released.

We propose that considering *humans as cognitive systems enacting in their socio-contextual environments* provides a framework for empowering them based on their sociocognitive needs, values, capabilities and limits. Using a human-centric perspective will not only enable designers and developers to consider the sociocognitive aspects of *consenting-agents* (i.e. end-users) in the development of new consent-obtaining mechanism, but can also provide a framework for evaluating the existing mechanisms designed to obtain consent on the Internet. In the latter case, which is how we use the developed basic human-centric perspective (presented in section 3), the human-centric framework can be used to evaluate whether an existing consent-obtaining mechanism (e.g. a cookies form) is able to empower end-users by considering different cognitive, collective, and contextual dimensions of the *consenting action* (i.e. giving consent as a multi-dimensional action) that is expected to be conducted via that mechanism. We propose that without considering a human-centric perspective, which considers the multi-dimensionality of human actions (or enactions), research or development on empowering technologies (including consent-obtaining mechanisms) is hardly an achievable task.

2.1 Fairness Matters: A Human-centric Perspective and Marginalized People

We propose that end-user empowerment using human-centric perspectives should be considered a universal approach in design, implementation, evaluation, and release

of consent-obtaining mechanisms for everyone. However, when marginalized and underprivileged people are concerned, the urgent need for a human-centric shift in design and implementation of consent-obtaining mechanisms becomes even more explicit: Marwick and Boyd [44] point out that while it is increasingly challenging for all individuals to maintain digital privacy due to our "networked age", it is even more challenging for people at the margins. They argue that people who are structurally and systematically oppressed (for example immigrants, LGBTQ+ communities, people of color) experience privacy differently than people with more privilege. Providing an example for such a scenario, they write that an ill person without adequate insurance who is seeking treatment will share their personal information much easier than a person with full health coverage.

Tene and Polonetsky [48] demonstrate a similar scenario wherein parent-children relationships can become strained due to privacy issues. They claim that parents have always tended to control their children's online activity. Until before the invention of parental filters that monitor and control every activity, children had the opportunity to shut the door and afford themselves some privacy. Given today's state of technology, the authors ask "what social norms constrain parents from persistently peering into their children's lives"? To describe how the "right to be left alone" is exercised in the current digital world, Marwick and Boyd [44] write that "as data-based systems become increasingly ubiquitous, and companies that people entrust frequently fail to protect personal data, the lines between choice, circumstance, and coercion grow increasingly blurry".

In order to manage their privacy in this ever less private digital world, people seek technological and social information. Therefore, people who are socially disadvantaged will presumably have a harder time maintaining their privacy [41]. Companies serving different demographics including very young and elderly people who are technologically less adept, could take advantage of these users. In a recent scandal involving Facebook's underage users, news reports in January 2019 stated that Facebook tried to increase its online gaming revenue by accepting payments from children unaware that their parents' credit cards were being charged [33]. In this predatory behavior, Facebook actively exploited children's lack of knowledge and refused to make proposed changes that could overcome the problem. Therefore, a "one size fits all" approach to privacy can be ignorant of social inequalities and in the worst case, it will allow for the exploitation of the least protected users.

The legal framework differentiates between data subjects, controllers and processors, but it would be a mistake to treat any of these groups as homogeneous, since data subjects have varying privacy attitudes [36], just as controllers and processors may collect different types of information for their services and products [39]. Although privacy is a legal right granted equally to citizens, the exercise of this right in real life conditions is usually more complicated and not everyone benefits equally from protection. We therefore propose that a human-centric perspective, wherein individual needs, values, capabilities, and limits of every single individual end-user is taken into account [30], is a significant aspect that needs to be considered in consent-obtaining digital mechanisms, as one of the most important information systems which are expected to protect human rights and values. Such human-

centric consent-obtaining mechanisms will not only empower privileged end-users but also empower and protect underprivileged and marginalized ones. If we consider the right to privacy as a basic human right and accept that consent-obtaining mechanisms need to be *fair* regarding the services they provide by respecting their users' needs, values, capabilities, and limits, human-centricity particularly gains prevalence.

3 Enacting Consent: *Consenting* as a Sociocognitive Action

In the previous section, we argued for a need for human-centric approaches towards consent-obtaining. In order to develop a basic human-centric framework for the evaluation of existing consent-obtaining mechanisms, we use one of the current paradigms in cognitive science, *enactivism* [32, 51]. This paradigm is supported by some of the most recent advancements and findings in cognitive science (see e.g. [5, 15]). According to enactivism, cognition arises through the continuous interaction of a cognitive system and its environment [51]. By taking an *enactivist perspective*, we propose that instead of reflecting on *consent* as a symbolic and abstract concept, we need to consider the *action* of *consenting* as one, which is the result of continuous and dynamic interactions between the end-user and the consent-obtaining system, performed in a social (and environmental) context. Based on this understanding, *consenting* is a sociocognitive action involving cognitive as well as social dimensions and processes.

Figure 1 provides a simple visualization of the sociocognitive dimensions of *consenting*. From an enactivist perspective, it is difficult to draw a line between different dimensions as they have overlaps. Moreover, all dimensions are in continuous interaction. Considering the state of the art in cognitive science (e.g. [32]) as well as the literature on digital privacy and current consenting behaviour of end-users, the *Social* dimension is divided into two ever-interacting and overlapping sub-

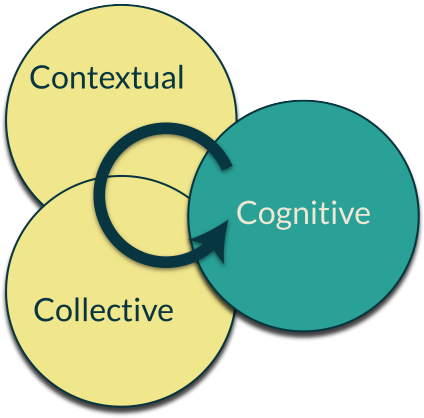

Fig. 1 A simple visualization of sociocognitive dimensions of *consenting*; The social dimensions are colored in Khaki.

dimensions, i.e. a *collective* dimension, and a *contextual* dimension. Collective refers to collective ownership of data, collective management of consents, and support of individuals regarding their privacy and consent-giving by other humans or communities. Contextual refers to contexts such as location, time, emotional-state, importance, etc wherein a consent is being given. Each of these dimensions are shortly discussed below in the specific context of consenting.

3.1 The Cognitive Dimension of Consenting

In an *ideal* world, everyone who agrees with using the same services should be protected digitally in the same ways but there appears to be a number of obstacles to attain this goal. The users, often treated as a homogeneous group, comprise agents with different needs, preferences, abilities, skills, knowledge and resources. As Marwick and Boyd [44] have recently discussed, maintaining privacy requires not just setting preferences on a digital service but also an active protection of information. Managing privacy by controlling when and where to share the information as well as who has access to the information is a difficult task. Users need increasingly complex technical and social skills to navigate these digital spaces, to assess the costs and benefits of their actions, and to strategically decide to share or hide information. In case of using consent-obtaining mechanisms, as they are implemented today, the users need to have a good understanding of their consent-related decisions (e.g. being able to consider their individual, contextual, and collective short and long-term consequences), as well as the ability to perceive and understand the visual elements of the user-interfaces, to eventually comprehend and make sense of the texts and information provided, among others, in the *terms of service*, *privacy policy*, and guiding documents.

Taking the complexity of consent-obtaining mechanisms into account, one may doubt a normal human-being's ability to perform these tasks, given the finite cognitive capacities and limited time, expertise, knowledge, resources, and so on. A detailed discussion of this subject exceeds the scope of this paper. It is, however, clear that *consenting* has a *cognitive* dimension, which should be taken into account. As proposed in literature [30], consent-obtaining mechanisms need to give consideration to humans' cognition and processes such as needs, values, capabilities and limits, if they aim at empowering them regarding the management of their privacy.

3.2 The Collective Dimension of Consenting

Lehtiniemi and Kortesniemi [37] note that people reveal information not only about themselves but also about others. They emphasise that "privacy self-management frames the decision-making on personal data as an individual choice based on

private cost-benefit analysis, despite personal data often also conveying information about others"[37]. For instance, when group photos or the location and time of events are posted on the Internet, people are publishing information about their peers as well. Subsequently, by downloading a mobile application that has access to the users' contacts, they are giving personal information away, which essentially belongs to other people. Considering that social data can be extracted from personal data and individual privacy decisions have social impacts, we must turn our attention to collective attitudes towards privacy protection.

Other aspects of the collective dimension of *consenting* include i.a. *peer-influence* and *expert-influence*. In a study conducted by Das et al. [17], the frequency of adoption of three Facebook security features by a group of 1.5 million users were analyzed. The results have shown that if a user has many friends, especially from different social groups, that have adopted a security feature, they are more likely to adopt that measure as well. In a more recent study conducted by Emami-Naeini et al. [19], 1000 online participants were asked about scenarios where the collection of personal data was allowed or rejected. In the study group, the researchers gave the participants information about the decisions of their peers and experts on the topic. In the control group, this information was not available. When participants were aware of the attitudes of other people, they were quicker to decide. This effect was larger in scenarios where the task was more difficult and required more time to decide. Granovetter [22](as cited in [38]) summarizes this point by proposing that "private cost-benefit decisions to disclose data are embedded in a network of social relations, and looking at them from an individuated, under-socialised point of view is misleading".

In summary, the collective dimension of consenting has different aspects: on the one hand, since many of the data types have collective privacy-related attributes (e.g. group photos), the consent associated with them, needs to be given (or obtained) in a collective manner; on the other hand, since 1) many of the people do not have enough expertise or abilities to manage their own privacy in an appropriate way, and 2) the social consequences of privacy invasion go beyond single individuals, people need to be supported by other peers and experts in their consenting and personal data management [8].

3.3 The Contextual Dimension of Consenting

Consenting, as a sociocognitive action, always happens within and in relation to contextual dimensions [35]. Time, location, emotions, other involved people, purpose, trust, urgency, contextual self-identity, and many other factors can influence the action of consenting. An individual from a specific social minority might have no issue with the processing of geographical information during the weeks while she is in her home city, but she might have serious concerns if the same data is collected while she is traveling on the weekend (e.g. due to potential consequences). The contextual aspect of human-centric perspective towards the development of

consent-obtaining mechanisms reminds us about at least two things: 1) providing fine-grained control possibilities for individuals, who are able to consider their own contextual specifications such as their situated needs, values, concerns, attitudes, capabilities, and limits; 2) perceiving *consent* as a contextual entity which should always be obtained in relation to contexts.

4 A Human-centric Evaluation of the GAFAM Practice of Consent Obtaining

Following the conceptualization of consenting as cognitive, collective and contextual *enactions*, we turn to the specific mechanisms of giving and obtaining consent in a online environment in the form of privacy options and cookie consent forms. The following sections investigate the nature of these three aspects of consenting in the context of the 'Big 5'–Google, Amazon, Facebook, Apple and Microsoft (GAFAM)–and their efforts to obtain end-user consent. The main reasons to choose above mentioned website are: 1) they are ranked among the websites with the highest numbers of users, 2) the enterprises running these websites not only have the legal obligations to obtain *lawful* consents from their diverse end-users (same as other websites), but also–as some of the most technologically advanced endeavors in the world–they posses sufficient resources to develop highly sophisticated consent infrastructures *if they choose to*, 3) they extensively use data subjects' personal data for a variety of purposes, including targeted advertising and profiling, which are specifically regulated by the GDPR. Starting with a critical analysis of web practices aimed at artificially increasing the cognitive load on the user, we investigate the process of giving and withdrawing consent for the use of private data, tracking cookies and targeted advertising.

4.1 Evaluating the Cognitive Aspect of Consenting

The process of giving or withdrawing consent in the digital space (i.e. digital consenting or online consenting) is becoming an increasingly difficult cognitive task. Not only is the potential amount of information to be disclosed growing massively, but the number of service providers and companies that are collecting data and thus are subject to the GDPR are also growing. Subsequently, users are confronted with the necessity to either accept the companies' terms of services *as-is* or to undertake the arduous task of choosing when to share which of their private data through web interfaces provided by the data collectors themselves, meaning privacy and cookie consent forms.

These forms are located in a paradox space between legal compliance and the interests of the company to collect as much data as possible on the one side, and the users' needs and rights to take control of their personal data, on the other. Therefore,

in this context, it seems plausible to assume that data controllers would not only first and foremost provide interfaces that are geared towards legal compliance, but also utilize design mechanisms in these digital consent mechanisms which are actively discouraging their own use. To answer just how common these presumed practices are is the empiric focus of our work, which we see as a necessary step towards establishing both the necessity and applicability of the framework presented before.

As described both in academic literature and by professionals in the web design industry [14, 23], a variety of design measures exist that are tailored to complicate interaction processes and increase the cognitive strain on the user, commonly referred to as *dark patterns*.

Dark patterns, a concept introduced by Brignull et al. in 2011, are

> *"[...] a type of user interface that appears to have been carefully crafted to trick users into doing things [where these user interfaces] are carefully crafted with a solid understanding of human psychology, and they do not have the user's interests in mind"* (Brignull et al., cited by Greenberg et al. [24, p. 2]).

To compare the utilization of such user interface design patterns in consent forms of the main webpages of the GAFAM, we utilize a taxonomy of these patterns introduced by Mathur et al. [45]: *Asymmetry*, *Covertness*, *Deceptiveness*, *Hidden Information* and *Restrictive Design*.

4.1.1 Methodology

In order to investigate the use of these patterns and discover other commonalities and discrepancies as well as subsequently evaluating the current practices in the context of our human-centric framework of consenting, we utilized a scenario-based critical interaction and design analysis as interpretative ethnography [7, 18]. Borrowing from Blackmon et al. [9], we asked usability and web design experts to conduct a *cognitive walkthrough* of the GAFAM cookie and privacy consent mechanisms to identify the above-mentioned dark patterns, conceptualizing them as usability problems.

For each of the five main web pages, this meant enacting a single user story: *"opt out of and withdraw consent for as many data collection and privacy practices as possible"*. Starting at the top-level-domain[1] for each company, we set the following goals:

1. Locate and document a cookie consent banner, notice or similar
2. Follow the available links to reach all available opt-out / consent withdrawal options
3. Document design patterns supporting or hindering the cognitive process of withdrawing consent

[1] To ensure the web page was specifically designed to be compliant with the GDPR, we chose the local top-level-domain of [blinded for review] where applicable. All consent forms mentioned the GDPR in one way or the other.

The process was completed separately by five experts in user interface design and information architecture in August 2019 while being observed and subsequently cross-validated by the authors to resolve discrepancies and questions. Choosing experts–with both industry and UI/UX research backgrounds–for this task in lieu of a larger, user-centric study allowed uncovering deeper design patterns and subtle mechanisms that average users might not be familiar with.

Each process was conducted using a pristine browser in "private" mode (with no cookies present prior to the process). When necessary, user accounts were created to explore the internal privacy options provided only for registered users. This allowed starting from a *tabula rasa* state for each web page, while also preserving the necessary cookie information as long as the session lasted. Given that the browsers utilized for the test[2] both prohibit the detection of whether or not the private mode was used–Chrome by default, Firefox through an extension–this approach was most promising in creating a pristine, comparable environment for each of the tests. No significant differences between the two browsers in regards to behavior or consent mechanism design were noticeable by the evaluators.

Evaluators were familiarized with the concepts of dark patterns and their taxonomy as described in the previous section prior to the cognitive walkthrough. Not all the evaluators reported the same patterns. However, during the ex-post discussions, the evaluators did not express any significant disagreement with the other evaluators' observations.

4.1.2 Results

While observing the process and documenting the observed design patterns, three aspects were particularly in focus: *interaction design*, *visual design* and *textual descriptions*. In terms of interaction design, the minimum amount of clicks and page jumps necessary to reach the required options, animation and hidden features (such as the 'read more' accordion or collapsible panel pattern [49]) received particular attention. For the visual design aspects, the size and location of interaction buttons were of primary importance, and the textual descriptions were compared throughout different pages in terms of the consistency of the description and terminology as well as their semantic relation to the interaction options (e.g. answering the question "Does the action promised by the 'opt-out' button correlate with the textual description underneath?"). Significant observations were collected and evaluated against the taxonomy of *dark patterns* noted above. The following analysis presents an overview of our findings.

Two overall distinctions emerge from our empiric analysis: first, only four of the five analysed sites (Amazon, Facebook, Google and Microsoft) make it *explicit*

[2] Firefox 68.0.1 and Chrome 76.0.3809 respectively

[3] Through third party tool

[4] Including Youtube

Table 1 Consent mechanism evaluation: key results

Company	Notice	Targeted Ads: Opt-Out	Shortest path (clicks)	Asymmetry	Covert	Deceptive	Information Hiding	Restrictive Design
Amazon	Explicit	Third-Party	10^3	Yes	Yes	Yes	Yes	Yes
Apple	Implicit	No	7	Yes	No	Yes	Yes	Yes
Facebook	Explicit	Third-Party	9^3	Yes	No	Yes	Yes	Yes
Google	Explicit	Yes	8 ($+3^4$)	Yes	Yes	Yes	Yes	No
Microsoft	Explicit	Yes	9	Yes	No	Yes	Yes	No

that users are giving consent to the use of their data in form of a cookie consent banner or a pop-up. Apple required looking for a footer link titled 'Use of cookies' in order to access information about collected data and find further links to the opt-out process. Second, not all the sites provide an opt-out option for users that either do not have an account or are not signed in. Specifically, Apple does not offer these options and instead urges users to sign in or create an account in order to set privacy preferences. Of the remaining four, Microsoft and Google allow opting out of targeted advertising through their own consent forms, and Amazon and Facebook only provide a link to three consent intermediaries–the *Digital Advertising Alliance*[5] (for the U.S.), *Digital Advertising Alliance of Canada*[6] and the *European Interactive Digital Advertising Alliance*[7]–which provide cookie-based opt-out settings that should span multiple third party websites and data collectors. While consent intermediaries promise some potential as alternatives to the privacy self-management model, Lehtiniemi et al. point out that they do not represent a solution to the underlying *"insuperable problems"* that stem from an individual-centric approach to privacy negotiation [38, p. 10].

Asymmetry describes a user interface design that *"[...] impose[s] unequal weights or burdens on the available choices [...]"* [45, p. 2], in most cases by subtle means, such as the size or placement of a preferred interaction (e.g. an 'Accept' button). It is worth noting that the default settings of all five web pages, in most cases, lie strictly in the interests of the data collectors, which assume end-users consent to any and all types of data collection and processing. In these data-controller-centric designs, the users are often expected to *actively opt out*.

With regards to specific user interface measures utilizing asymmetrical patterns, Facebook prompts a large *'Accept'* button for its terms of service agreement next to a comparatively small *'See my options'* link upon logging in. Google's interface design, at first, seems to try to nudge the user to *'Review Now'* their pop-up titled *'A privacy reminder from Google'*, with the only other option being *'Remind me later'*; in the following review window, the *'Accept now'* button is prominently placed next to a more subdued *'Other Options'* button (see Figure 2). Both examples

[5] `http://optout.aboutads.info/`

[6] `https://youradchoices.ca/`

[7] `http://www.youronlinechoices.eu/`

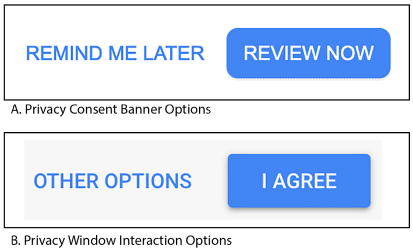

Fig. 2 Asymmetric choices in Google's consent banner and forms.

illustrate a strategy of presenting two interaction choices in a graphical way that suggest user a binary, *either-or* decision ('I consent' vs. 'I do not consent'), which in reality represent separate, non-binary functionalities (such as 'consenting' vs. 'exploring other options'). This strategy exploits a user's cognitive bias by violating expectations of regularity [25] and increases the cognitive strain to accomplish the task of withdrawing consent.

Covertness patterns aim at hiding the effects of a user's choice in order to steer them into a certain direction. Not all consent form interfaces employ this strategy *per se*, but they may exploit similar effects that can be subsumed under *'covertness'* strategies. Amazon, for instance, allows users to opt out of *'interest-based ads'*, but informs them in the small print underneath that *"[e]ven if you choose not to see interest-based ads, you may still see personalised product recommendations and other similar features unless you've adjusted Your Recommendations in your Account Settings or Your Browsing History"* [1]. The link to *"Account Settings"* leads the user to a page listing their recent purchases. In that page, the user can choose manually (and one by one) to exclude their purchases from being employed for further recommendations, but no 'reject all' button is provided. *'Your browsing history'*, on the other hand, presents a similar list that shows recently viewed items and does provide an option for removing all items from the history, and turn off the browsing history tracking all together, though both options are hidden behind a *'Manage history'* button. The multitude of different interaction methods complicates the cognitive process of comprehending the available choices and their effects. Also, it can be subsumed under covertness strategies. Similarly, Microsoft's opt-out page for personalized ads only mentions data utilization for personalization, but not data collection itself [2]. Only through the long-form help pages on *'How to access and control your personal data'* [3] the user is informed that opting out of ad personalization does not stop the data collection, and that the execution of their rights to data sovereignty as mandated by the GDPR will require contacting Microsoft via email or another form (but it does not allow an automated opt-out).

While some of the *covertness* strategies of complicating the process exemplified above represent a more subtle way of dark pattern design, a number of interface design choices are obviously misleading and leave the impression of purposeful *deceptiveness*. Google's consent pop-up, for instance, presents the following 'tip':

"When you sign in with your Google Account, you can control what's saved to your account and manage past searches." The language used suggests that signing in with an account might actually increase one's control over the data collected, while omitting the fact that signing in also increases both the amount of (meta-)data collected and its value within the culture of surveillance capitalism that ad-revenue dependent companies like Google thrive in [40]. Another example is Microsoft's *'Privacy Statement'* [3], which users reach by clicking on a cookie consent banner presented at `microsoft.com`. This link leads to the section for *'Cookies or similar technologies'*, which in general terms explains what cookies are and how they are used by Microsoft. The paragraph concludes:

> *"You have a variety of tools to control the data collected by cookies, web beacons, and similar technologies. For example, you can use controls in your internet browser to limit how the websites you visit are able to use cookies and to withdraw your consent by clearing or blocking cookies."*

Notably, this does not mention any opt-out functionalities to withdraw consent. Underneath the paragraph, a small *'Learn more'* link opens a much more detailed long-form version of this short paragraph, which includes a reference to *'Interest-based advertising'*, which leads the user to yet another summary on the same page titled *'How to access and control your personal data'*. Here, finally, the user can find a link to the general opt-out page for targeted advertisements as well as a link to the Microsoft privacy dashboard for users with a Microsoft account. Even here, after disclosing the link to the opt-out page, the corresponding *'Learn more'* link leads to a much longer list of Microsoft products collecting and utilizing personal data (such as Microsoft Cortana, Skype, or the Microsoft Store) and the respective links to control privacy settings and data collection. The numerous redirecting links and hidden pages suggest that the goal of this page is not to empower the users to control their (implicitly assumed) consent, but to keep all but the most persistent users from finding and executing their right to withdraw consent for data collection and utilization.

A dark pattern that is employed by all GAFAM companies is *Hidden Information*. Functionalities that allow users the opt-out from data-collection practices are often obscured through lengthy texts, multiple pages, synonymous descriptions and terms or they are visually hidden and require specific interaction to be found. Microsoft's *'Privacy Statement'* and its hidden paragraphs and Amazon's distribution of privacy controls over 4 different pages are just two examples of overly convoluted information architecture and design. Vague language on which personal data are collected and which personal data are required to provide the services, and a reluctance to clarify the difference between data collection and utilization (in the case of targeted ads, for instance) can be found consistently throughout the privacy and consent mechanisms of all five company ecosystems.

One specific example of particular obfuscation is Apple's privacy information page: a lengthy text explains Apple's use of targeted ads in its Apple News and App Store products and informs the user of *'Limit Ad-Tracking'* in order to opt-out of this feature. There is no direct link to any settings page that allows this. The text also

does not mention that this setting is only available on Apple devices like iPhone, iPad, or Apple TV. It means that the users themselves need to find the instructions on Apple's support pages.

Finally, *Restrictive Design* plays a role for all five companies. A tendency to initially push the responsibility for opt-out of tracking, data collection and targeted advertising towards the user by suggesting browser-based measures to block cookies as a first solution can be observed in all cases. The fact that this inevitably leads to restrictions not only in the use of the webpage in question, but *any* webpage that requires cookies to function, can be seen as leverage against this global opt-out. Three of the five companies (Amazon, Apple and Facebook) explicitly mention that blocking cookies would prevent the user from using certain parts of their sites, but Apple and Facebook remain vague about the exact nature of these restrictions. Only Amazon clarifies:

> *"[...] if you block or otherwise reject our cookies, you will not be able to add items to your Shopping Basket, proceed to Checkout, or use any Amazon Services that require you to Sign in"*

The combination of primarily suggesting that users who are privacy conscious should block all cookies, and the reluctance to provide clear instructions and fine-grained control over which type and use of cookies the user consents to, results in an underlying theme of coercing the user towards giving consent to all data use.

5 Discussion

5.1 Dark patterns and the assault on the cognitive dimension of consenting

Considering the empirical results, little evidence has surfaced that suggest the GAFAM web pages were designed with a human-centric perspective to empower users to give their informed consent. On the contrary, the nature of the techniques employed suggest that empowering users is not the main focus of these consent mechanisms. Patterns of coercion that nudge the user towards consenting, strategies of information hiding, covert and confusing interface behavior have been shown to exploit human cognitive weaknesses more than supporting the complex process of consenting to a multitude of data collection and utilization [10, 14]. Current research literature (e.g. [5, 32]) from the cognitive sciences supports the theory that the high-level patterns we observed have an adverse effect on the cognitive efforts involved in enacting consent through the mechanisms studied, as detailed in section 3.1.

5.2 The Missing Aspects: Collectiveness and Contextuality

Current approaches to privacy management presume that users are informed and capable of deciding these matters individually. As we've discussed, this perspective ignores that many users find privacy policies complex and the fact that the decisions of other people influence individual users.

Empowering end-users should not only aim at overcoming the mechanisms that actively discourage the end-users from the withdrawal of their consents or push them to choose specific types of consent. A human-centered approach should also regard the collective dimension of consenting–an aspect for which the existing solutions provide no support at all. For instance, the difficulties of grasping the complex technical consequences of consenting to targeted ads might be alleviated by presenting the users with expert opinions on what their potential choice entails, or by providing an overview of choices by comparable peers. Friends, family members, peers, trusted enterprises or even trusted AI systems can support users in managing their online consent and tracking decisions.

Furthermore, the current model of individual consent stands in stark contrast with the very broad, all-encompassing options presented to the user–in some cases even simply blocking any and all cookies, which often results in the exclusion from a variety of services implemented to be dependent on the use of cookies. Such 'one-size-fits-all' approaches to consenting or objecting, ignore the heterogeneous contexts and multiplicity of the human experience, and represent another coercive strategy to encourage the user to engage in the bargain of consenting to *everything* to get *something*. A human-centric approach to consent would thus imply providing users with more fine-grained controls: this approach would not only include the question of *what* the user consents to share, but also the time, location or other contextual information. As mentioned in section 2.1 for instance, a user might be willing to share certain information while at home, but withdraw that consent while working on sensitive information at their office. Similarly, users might generally consent to the use of targeted ads, but want an emergency opt-out mechanism in case of a personal crisis. Considering some of these contextual dimensions could alleviate the strain that the implicit, 'always on' consent approach puts on members of marginalized populations.

Finally, although some of the consent-obtaining systems are quite elaborate in terms of interaction and visual design, none of the surveyed systems utilized any other type of informing users but lengthy textual descriptions of their data and privacy practices. Since the legal framework provided by the GDPR does not specify the nature of how users should be informed, one answer to the heterogeneous needs of a diverse user base should be the presentation of information relevant to the consenting actions in different forms. For instance, animations, video explanations, interactive visualizations, or *negotiation-based* interactive approaches (combined with personal privacy management systems) can be used to reach a diverse audience and could address the contextual dimension of enacting consent on a more individual level. Moreover, pluralist approaches to knowledge representation (see e.g. [28, 27])

can be used to represent privacy-related information to end-users based on their diverse needs.

5.3 Fairness, Accountability, and Transparency of GAFAM consent-obtaining mechanisms

Evaluating these current approaches to consenting shows obvious shortcomings with regards to transparency. On the one hand, the use of patterns like *covertness* or *hidden information* directly contradicts standards of transparency and disclosure regarding the data utilization practices employed by the data-collectors. On the other hand, the common practice of providing extensive texts to explain data use and the company's privacy policy in the name of transparency leads to little more than burying few relevant pieces of information–for instance, instructions on how to withdraw consent or adapt it. Referring to the issue of the language used in explaining the practices and available options to the users, as Kemper [34] argues, transparency alone is not enough to provide a greater accountability of such systems: without a *critical audience*, accountability remains an *'empty signifier'*. But even with an engaged critical audience, it is highly questionable that this kind of transparency automatically leads to a greater amount of accountability of such systems either: these strategies of over-disclosing would qualify as *'opaque transparency'*, according to Fox [21].

Another dimension of transparency in the consent-obtaining mechanisms concerns user feedback on the choices made. In this case, transparency is a necessary precondition for accountability: if there are no ways for the users to see concrete evidence of the effect of their choices, the resulting system can hardly be described as accountable. Given the increasingly subtle mechanisms of targeted advertising and the fact that, even after an opt-out, ads might still be tailored to the users based on intermediate activities without data collection or processing that would fall under the regulations in the GDPR [20], it might be increasingly difficult for a user to tell the difference their choice made. Illustrative examples and more transparent traceability of data-collection related activities–similar to the "Why am I seeing this ad?" utilized by Facebook–might provide illumination in these cases.

As discussed in section 2.1, any implementation of privacy and consent-obtaining mechanisms carries the danger of affecting members of marginalized groups negatively in disproportional numbers if the implementation does not consider the context of the user. The current examples seem woefully lacking in this regard, as explained above. As long as the consent-obtaining mechanisms and their implementations are framed within the perspective and goals of the data controllers (i.e., the company providing services in exchange for data collection), fairness in privacy will not improve, but may be actively compromised.

Finally, given that obtaining consent is just one of the various legal bases for a lawful practice of data processing as outlined by article 6 of the GDPR [20], it

stands to reason that–should consent be used to justify data processing over other options–companies should be held accountable for the way they elicit that consent.

5.4 Lawfulness of Non-human-centric Consent-obtaining Mechanisms?

While this paper does not aim at proposing any legal claim, a basic reflection on the potential legal implications of our human-centric framework can be helpful for other researchers. According to the GDPR (in particular Art. 6 [20]), end-user consents, if obtained, need to be *valid*, *freely given*, *specific*, *informed* and *active*. Considering our evaluation of *cognitive* dimensions of *consenting*, the justification of the obtained consents, as practiced by GAFAM, as *valid*, *freely given*, *specific*, *informed* and *active* seems very difficult from a human-centric perspective. As a result, one can raise doubt regarding the lawfulness of these practices from a human-centric perspective.

Moreover, given the fact that based on the GDPR, the data processing purposes and the privacy policies of data-controllers must be *understandable* for the end-users–in case of obtaining their consents at least–one can question the willingness and attempts of GAFAM to develop *understandable* consent-obtaining mechanisms. Furthermore, since the GDPR allows complementary approaches such as visualizations, an open question would be why these data-controllers do not use other means such as videos, animations or interactive media in their consent-obtaining mechanisms.

6 Limitations & Future Work

The basic human-centric framework presented in this paper provides many potential research directions that we aim at following in the next steps. Given the state of the art in cognitive science and in particular, the *predictive processing* [32] account of cognition, we aim at conducting empirical experiments on the cognitive aspects of consenting in different social groups. Moreover, we aim at developing a simple collective consent management prototype and evaluate how this could support marginalized people to deal with their privacy on the Internet.

Regarding our GAFAM evaluation, the study is limited by both it's scope and methodology; a further empirical and user-centric evaluation to verify the specific impact of the observed patterns on cognitive load (and on the other aspects of human cognitive systems), including the collection of quantitative evidence such as site structure, or tree-analysis of the necessary steps as well as timed scenarios could provide further proof for the lack of human-centricity in the current implementations. Additionally, the study of region-specific or social group-specific differences as well as a separate evaluation of consent mechanism behavior on

mobile devices was outside the possible scope of this study as well, which could yield further insight into the landscape of consent-obtaining mechanisms at large.

Nevertheless, the results of the current study are sufficient to be used to design and conduct a user-based evaluation study of the target consent-obtaining (and consent-management) mechanisms. Moreover, we aim at conducting a set of qualitative and user-based evaluations on consent-obtaining intermediaries (cookies consent forms) and comparing the existing solutions from a human-centric perspective. Furthermore, we hope to be able to conduct more in-depth research on the potential legal consequences of our proposed human-centric approach. Finally, we propose that more research on the socioeconomic aspects of consent-obtaining mechanisms, such as the business models of the involved enterprises as well as the consequences of the current practices are needed.

7 Conclusion

In this research, we proposed a shift towards human-centric end-user empowerment regarding obtaining digital consent. We argued that based on the recent advancements in cognitive science, *consenting* needs to be considered a sociocognitive action. Such action includes dynamically interacting *cognitive*, *collective*, and *contextual* dimensions that should be taken into account in the design and implementation of consent-obtaining mechanisms and consent management systems. Based on the developed framework, we evaluated the mechanisms of consent-obtaining in GAFAM's main websites. Our results show that the collective and contextual aspects are almost completely ignored in their design. Moreover, we showed that human-centric cognitive dimensions of consenting are not only used in a positive manner–which could lead to end-user empowerment–but also have been suppressed by implicit dark patterns which need to be avoided.

While we are aware that further research is needed on how the developed framework can be used to design and implement new mechanisms (not just the evaluation of the existing ones), we still think that the developed basic framework can provide a useful evaluative approach for consent-obtaining mechanisms. Finally, we propose that while many of the legal frameworks (such as the GDPR) follow a very individual-centric approach towards *consenting*, considering different aspects of *collective* and *contextual* dimensions of *consenting* in design and implementation of consent-obtaining mechanisms (and consent-management systems) can highly contribute to human empowerment in the digital era.

8 Acknowledgement

This work is partially funded through the EXPEDiTE project (Grant 867559) by the Austrian Federal Ministry for Climate Action, Environment, Energy, Mobility,

Innovation and Technology under the program “ICT of the Future” between September 2018 and February 2020.

We would like to express our great appreciation for valuable criticism and ideas contributed by Gustaf Neumann, Seyedeh Anahit Kazzazi, Seyedeh Mandan Kazzazi, Stefano Rossetti, Kemal Ozan Aybar, Rita Gsenger, and Niklas Kirchner.

References

1. Amazon.de: Advertising Preferences (2019). URL $https://www.amazon.de/adprefs?ref_=ya_d_l_advert_prefs$. [Online; accessed 22. Aug. 2019]
2. Microsoft account | Privacy (2019). URL https://account.microsoft.com/privacy/ad-settings/signedout?ru=https:%2F%2Faccount.microsoft.com%2Fprivacy%2Fad-settings. [Online; accessed 23. Aug. 2019]
3. Microsoft Privacy Statement – Microsoft privacy (2019). URL https://privacy.microsoft.com/en-us/privacystatement. [Online; accessed 23. Aug. 2019]
4. Acquisti, A.: Privacy in electronic commerce and the economics of immediate gratification. In: Proceedings of the 5th ACM conference on Electronic commerce, pp. 21–29. ACM (2004)
5. Allen, M., Friston, K.J.: From cognitivism to autopoiesis: towards a computational framework for the embodied mind. Synthese **195**(6), 2459–2482 (2018)
6. Alt, R., Human, S., Neumann, G.: End-user empowerment in the digital age. In: Proceedings of the 53rd Hawaii International Conference on System Sciences, pp. 4099–4101 (2020)
7. Anderson, R.J.: Representations and Requirements - The Value of Ethnography in System Design. Human–Computer Interaction **9**(2), 151–182 (1994). DOI 10.1207/s15327051hci0902_1
8. Aybar, K.O., Human, S., Gesenger, R.: Digital inequality: Call for sociotechnical privacy management approaches. Workshop on Engineering Accountable Information Systems. European Conference on Information Systems - ECIS 2019 (2019)
9. Blackmon, M.H., Polson, P.G., Kitajima, M., Lewis, C.H.: Cognitive walkthrough for the web. CHI p. 463 (2002). DOI 10.1145/503376.503459
10. Bösch, C., Erb, B., Kargl, F., Kopp, H., Pfattheicher, S.: Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns. Proceedings on Privacy Enhancing Technologies **2016**(4), 237–254 (2016). DOI 10.1515/popets-2016-0038
11. Boyd, D.: It’s complicated: The social lives of networked teens. Yale University Press (2014)
12. Boyd, D., Marwick, A.: Social privacy in networked publics: Teens attitudes, practices, and strategies. In: Decade in Internet Time: Symposium on the Dynamics of the Internet and Society. Oxford, UK (2011)
13. Busch, A.: Privacy, technology, and regulation: why one size is unlikely to fit all. Social dimensions of privacy: interdisciplinary perspectives. Cambridge University Press, Cambridge pp. 303–323 (2015)
14. Chromik, M., Eiband, M., Völkel, S.T., Buschek, D.: Dark Patterns of Explainability, Transparency, and User Control for Intelligent Systems. IUI Workshops **2327** (2019)
15. Clark, A.: Whatever next? predictive brains, situated agents, and the future of cognitive science. Behavioral and brain sciences **36**(3), 181–204 (2013)
16. Commission, E.: Special eurobarometer 431: Data protection (2015)
17. Das, S., Kramer, A.D., Dabbish, L.A., Hong, J.I.: The role of social influence in security feature adoption. In: Proceedings of the 18th ACM conference on computer supported cooperative work & social computing, pp. 1416–1426. ACM (2015)
18. Dourish, P.: Implications for design. In: the SIGCHI Conference, p. 541. ACM Press, New York, New York, USA (2006). DOI 10.1145/1124772.1124855

19. Emami Naeini, P., Degeling, M., Bauer, L., Chow, R., Cranor, L.F., Haghighat, M.R., Patterson, H.: The influence of friends and experts on privacy decision making in iot scenarios. Proceedings of the ACM on Human-Computer Interaction **2**(CSCW), 48 (2018)
20. EU: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing. Official Journal of the European Union pp. 1–88 (2016)
21. Fox, J.: The uncertain relationship between transparency and accountability. Development in Practice **17**(4-5), 663–671 (2007). DOI 10.1080/09614520701469955
22. Granovetter, M.: Economic action and social structure: The problem of embeddedness. American journal of sociology **91**(3), 481–510 (1985)
23. Gray, C.M., Kou, Y., Battles, B., Hoggatt, J., Toombs, A.L.: The dark (patterns) side of UX design. In: Conference on Human Factors in Computing Systems - Proceedings. Purdue University, West Lafayette, United States (2018). DOI 10.1145/3173574.3174108
24. Greenberg, S., Boring, S., Vermeulen, J., Dostal, J.: Dark patterns in proxemic interactions - a critical perspective. Conference on Designing Interactive Systems pp. 523–532 (2014). DOI 10.1145/2598510.2598541
25. Huber, J., Payne, J.W., Puto, C.: Adding Asymmetrically Dominated Alternatives: Violations of Regularity and the Similarity Hypothesis. Journal of Consumer Research **9**(1), 90–98 (1982)
26. Human, S., Bidabadi, G., Peschl, M.F., Savenkov, V.: An enactive theory of need satisfaction. In: V.C. Müller (ed.) Philosophy and Theory of Artificial Intelligence 2017, pp. 40–42. Springer International Publishing, Cham (2018)
27. Human, S., Bidabadi, G., Savenkov, V.: Supporting pluralism by artificial intelligence: Conceptualizing epistemic disagreements as digital artifacts. In: V.C. Müller (ed.) Philosophy and Theory of Artificial Intelligence 2017. Springer, Cham (2018)
28. Human, S., Fahrenbach, F., Kragulj, F., Savenkov, V.: Ontology for representing human needs. In: P. Różewski, C. Lange (eds.) Knowledge Engineering and Semantic Web, pp. 195–210. Springer International Publishing, Cham (2017)
29. Human, S., Gsenger, R., Neumann, G.: End-user empowerment: An interdisciplinary perspective. In: Hawaii International Conference on System Sciences 2020, pp. 4102–4111 (2020)
30. Human, S., Neumann, G., Peschl, M.: [how] can pluralist approaches to computational cognitive modeling of human needs and values save our democracies? Intellectica (70), 165–180 (2019)
31. Human, S., Wagner, B.: Is informed consent enough? considering predictive approaches to privacy. In: CHI2018 Workshop on Exploring Individual Differences in Privacy. Montréal (2018)
32. Hutto, D.D.: Surfing uncertainty: Prediction, action and the embodied mind, by andy clark: New york: Oxford university press, 2016, pp. xviii+ 401,£ 19.99 (hardback). (2018)
33. Kain, E.: Facebook Turned A Blind Eye To 'Friendly Fraud' As Kids Racked Up Thousands On Games. Forbes (2019)
34. Kemper, J., Kolkman, D.: Transparent to whom? No algorithmic accountability without a critical audience. Information, Communication & Society **0**(0), 1–16 (2018). DOI 10.1080/1369118X.2018.1477967
35. Kirchner, N., Human, S., Neumann, G.: Context-sensitivity of informed consent: The emergence of genetic data markets. Workshop on Engineering Accountable Information Systems. European Conference on Information Systems - ECIS 2019 (2019)
36. Kumaraguru, P., Cranor, L.F.: Privacy indexes : a survey of Westin's studies (2005). DOI 10.1184/R1/6625406.v1
37. Lehtiniemi, T., Kortesniemi, Y.: Can the obstacles to privacy self-management be overcome? exploring the consent intermediary approach. Big Data & Society **4**(2), 2053951717721,935 (2017)

38. Lehtiniemi, T., Kortesniemi, Y.: Can the obstacles to privacy self-management be overcome? Exploring the consent intermediary approach. Big Data & Society **4**(2), 205395171772,193 (2017). DOI 10.1177/2053951717721935
39. Lupton, D.: Personal data practices in the age of lively data. Digital sociologies pp. 335–50 (2016)
40. Lyon, D.: Surveillance capitalism, surveillance culture and data politics pp. 1–15 (2018)
41. Madden, M.: Privacy, security, and digital inequality: How technology experiences and resources vary by socioeconomic status, race, and ethnicity. Data & Society, Sep (2017)
42. Marwick, A., Fontaine, C., Boyd, D.: "nobody sees it, nobody gets mad": Social media, privacy, and personal responsibility among low-ses youth. Social Media+ Society **3**(2), 2056305117710,455 (2017)
43. Marwick, A.E., Boyd, D.: Networked privacy: How teenagers negotiate context in social media. New media & society **16**(7), 1051–1067 (2014)
44. Marwick, A.E., Boyd, D.: Privacy at the margins| understanding privacy at the margins—introduction. International Journal of Communication **12**, 9 (2018)
45. Mathur, A., Acar, G., Friedman, M., Lucherini, E., Mayer, J., Chetty, M., Narayanan, A.: Dark Patterns at Scale - Findings from a Crawl of 11K Shopping Websites. CoRR **1907**, arXiv:1907.07,032 (2019)
46. Obar, J.A., Oeldorf-Hirsch, A.: The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services. Information, Communication & Society pp. 1–20 (2018)
47. Rudolph, M., Feth, D., Polst, S.: Why users ignore privacy policies–a survey and intention model for explaining user privacy behavior. In: International Conference on Human-Computer Interaction, pp. 587–598. Springer (2018)
48. Tene, O., Polonetsky, J.: A theory of creepy: technology, privacy and shifting social norms. Yale JL & Tech. **16**, 59 (2013)
49. Tidwell, J.: Designing Interfaces. Patterns for Effective Interaction Design. "O'Reilly Media, Inc." (2005)
50. Van Dijck, J., Poell, T., De Waal, M.: The platform society: Public values in a connective world. Oxford University Press (2018)
51. Varela, F.J., Thompson, E., Rosch, E.: The embodied mind: Cognitive science and human experience. MIT press (2017)
52. Zuboff, S.: The age of surveillance capitalism: The fight for a human future at the new frontier of power. Profile Books (2019)