seminar.net
MEDIA, TECHNOLOGY & LIFELONG LEARNING
www.seminar.net

ISSN: 1504-4831 Vol 17, No 2 (2021) https://doi.org/10.7577/seminar.4291

A feminist Critique to digital consent

Elinor Carmi
University of Liverpool
Email: Elinor.Carmi@liverpool.ac.uk

Abstract

This paper presents a feminist critique to digital consent and argues that the current system is flawed. The online surveillance adtech industry that funds the web developed a mechanism that commodifies people, rendering their behaviors into data - products that can be sold and traded for the highest bidder. This was made possible by objectifying, dehumanizing and decontextualizing human engagement and identity into measurable and quantifiable data units. In this context, digital consent serves as an authorizing and legalizing instrument to the exploitative business model of spying, selling and trading people in the online ecosystem. Using four key feminist approaches - process, embodiment, network and context - this article shows the way digital consent is a mechanism that transfers responsibility to people and enables an exploitative-extractivist market to exist. The design of digital consent creates a specific interface that teaches people to behave in ways that preserve these asymmetric power relations. Consequently, the article shows the broader educational impacts of digital consent, which conceive people as products with narrow agency and understanding of what they can do, think and imagine. The article concludes with a refusal to provide an easy solution to a flawed system.

Keywords: Digital consent, feminist critique, surveillance capitalism, network, process, embodiment, context.

Introduction

At the end of the 1990s and the beginning of the 2000s, advertisers quickly realized that audiences would not pay for internet content or services, and therefore moved to a different business model to fund the web, in which people's behaviors would become the main currency (Turow, 2012: 37). Instead of paying to get content and services, people's behavior would be measured, packaged as profiles/audiences and traded between different

entities such as publishers, advertising networks and data brokers. All these procedures and online markets have been functioning in the backend, thanks to web browsers' interface design and default settings, without people's knowledge (Carmi, 2020a). This new online and hidden market introduced new communication channels and ways to produce the body and how it behaves within these privatized spaces. To establish how this new relationship will be defined, operated and regulated, new types of contracts were introduced. An important type of contract to authorize this new business model was the digital consent mechanism, where people, mainly in the European Union, had to indicate they consented to having 'their data' processed to be able to access free services.

Displayed in various ways, digital consent mechanisms ask people to express their agreement to being spied on throughout time, to the creation of multiple profiles by entities they are not familiar with and to being traded for the highest bidder in real-time-bidding. As the sociologist Zeynep Tufekci argues in relation to the Facebook Cambridge Analytica data exploitation incident: "Given this confusing and rapidly changing state of affairs about what the data may reveal and how it may be used, consent to ongoing and extensive data collection can be neither fully informed nor truly consensual — especially since it is practically irrevocable" (2018). In other words, digital consent does not work for us, but it does work for the corporations that are involved in this online ecosystem.

While legal, ethical and design academics have been debating on what is the best way to display and operationalize consent on different digital platforms and services, few have asked a much bigger question - Why do we have digital consent to begin with? This paper seeks to answer this question by using feminist critique to uncover the power asymmetries involved in digital consent. It highlights why cosmetic changes to digital consent in the shape of interface design will not change the problem. The article argues that design debates to create more 'ethical' consent mechanisms strengthen the current exploitative business model by legitimizing and normalizing the broken ecosystem that it relies on. The paper also focuses on how the architecture that has incorporated digital consent creates long-term consequences for the way people understand and think about data-driven technologies.

In order to understand why digital consent is a flawed mechanism, I will use four key feminist approaches that will amplify how digital consent is used *against* people and not *for* people. These concepts are: process; embodiment; network; and contextuality. In the following sections, I first discuss what the political economy behind digital consent consists of, highlighting the design of the adtech online ecosystem and Shoshana Zuboff's Surveillance Capitalism concept. In the next section, I highlight the debates of legal and design scholars around consent. Here, I will show how within these fields the discussions and arguments operate within the normative boundaries of digital consent without questioning whether it is a suitable and legitimate tool. I then move to discuss the four key feminist concepts and how they help us to rethink digital consent and point to its

exploitative nature. Next, I move to show what are the educational consequences of digital consent mechanisms. Finally, I conclude by a call for action and refusal to consent to the current situation.

The political economy of digital consent

Legally binding informed consent first appeared in 1957 in the biomedical field in the decision Salgo v. Leland Stanford, where the court had to decide whether a patient was given the appropriate information before a medical procedure. As Daniel Lin and Michael Loui (1998) argue, by the 1970s and 1980s, different human rights groups from civic, gender and consumer spheres had included and promoted the issue of informed consent in their agenda. Applying 'consent' as an ethical mechanism in different social relations is used to challenge the asymmetric power dynamic in different life spheres and give the individual more agency on choices that affect their bodies and lives. Importantly, consent has been introduced in various spheres of life as a social-legal contract for people to have more control, agency and autonomy on their bodies and lives.

From the 1990s, people's lives have been augmented into the digital environment of the internet and world-wide-web. This also introduced new types of social relations which necessitated new types of contracts. During the 1990s, as mentioned above, a different business model started to emerge, in which people and their behaviors became the product, which can be characterized as *surveillance capitalism* (Zuboff, 2015) or *data capitalism* (Myers-West, 2019). Surveillance capitalism, as Zuboff calls it, is a new type of information capitalism that aims to predict and change human behavior to produce revenue. One of the key stages that Zuboff identifies is 'extraction' which is:

> A one-way process, not a relationship. Extraction connotes a 'taking from' rather than either a 'giving to,' or a reciprocity of 'give and take.' The extractive processes that make big data possible typically occur in the absence of dialogue or consent, despite the fact that they signal both facts and subjectivities of individual lives. These subjectivities travel a hidden path to aggregation and decontextualization, despite the fact that they are produced as intimate and immediate, tied to individual projects and contexts (Zuboff, 2015: 79).

But how does this 'extraction' happen? And what type of relationship does this new adtech ecosystem create? When a person types the address of, for example, *The Guardian*, the server of that publisher will send her the things that she asked for which will appear on her screen in the shape of images, texts and videos. But at the same time, and thanks to browsers' default settings, *The Guardian's* server will also send her web-cookies. Unlike the common definition of web-cookies as 'just text files', I argue elsewhere that they "are (bulk) communications conducted by non-human actors (users' browsers and publishers or advertising networks) who 'talk' with each other about predefined 'topics' (specific behavior of people), and create 'a flow of communication back and forth between that hard

drive and the website's server" (Carmi, 2017: 294). Your behavior, preferences, location, broadband connection etc. become the message – the data – that is being communicated between your device and the server. This is all conducted at the backend of your screen, concealed behind nicely designed interfaces which make it impossible for you to know this is happening. In other words, *the person* becomes the message in an online market operating multiple silent communication channels trading and bidding her data in the backend of her screen.

When cookies are sent from the server of the address that a person typed in the address bar they are called first party cookies, and when cookies are sent from other companies such as data brokers and advertising networks, they are called third party cookies. The amount of cookies sent to a person's device is so huge it is hard to grasp, not one or two or even 10 companies, but rather hundreds and thousands of companies (for a good discussion and visualization check [Christl, Kopp, and Riechert, 2017]).

Many people find it difficult to imagine what is happening to their data, but it is similar to hundreds of electrodes connected to a person's body without their knowledge by companies they do not even know, that track, measure, record and store their every movement. The kind of 'data', or topics that are communicated on your behalf can be many types, like the browser you are using, your gender, location, age, religion, health, sexual orientation, musical preferences, what you do on multiple websites, apps and games and much more. All of this is happening in an *ongoing process* and it is not always clear how much of 'you' (data) is being communicated and for how long (Carmi, 2020a). It is also not clear which parts of a person (rendered as data), are being used and how, by these companies when they store and trade you. In addition to using data extracted from people to create multiple profiles and audiences, these data brokers also bid on people and the type of content, connections and behaviors they should engage with through an online bidding system called real-time-bidding (Carmi, 2020b).

As Zuboff argues, our subjectivities are converted into data objects that transform our subjective self into a commodity that can be packaged and repackaged as profiles and audience segmentations. As part of this conversion, there is a process that Zuboff terms as an 'un-contract' because contracts move from the social context to a computer mediated process in which people are deprived from consensual participation, free will and protection of their rights. As David Lyon argues, in surveillance capitalism "[t]here is no transaction with users or consumers, however. Straight extraction is all that occurs at that level. The trade in data is entirely between large corporations" (Lyon, 2019: 67). This extractive relationship also involves experimentations to modify people's behavior with the intention to monetize these interventions for profit and control.

Similarly, data capitalism, as Sarah Myers-West argues, "places primacy on the power of networks by creating value out of the digital traces produced within them" (Myers-West,

2019: 2). But it is not simply 'traces' which gives a passive sense of 'leftover data', as she argues, it is a special surveillance ecosystem designed to forcefully extract behaviors in a covert way. This novel form of capitalism relies on the monetization of productive intimacies between people and their machines. This new type of relationship creates asymmetric power where people provide both the labor and at the same time the currency/product of trade by being spied on continuously.

In this new online economy, consent is meant to 'empower' and give us 'control' over 'our' data by indicating whether we agree or disagree to procedures of 'processing' of this data. Processing, according to the European Union's General Data Protection Regulation (GDPR) that came into force in 2018, "means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction" (European Parliament, 2016). As this definition shows, there are around 17 different procedures that processing can include and some of them can be conducted in conjunction with others. So, when we indicate that we 'consent' before we upload a webpage or use a service there are many possible procedures that can be applied to us. We also do not know which parts of us, which pieces of extracted data are being processed. The common argument is that if we just have the right amount of information about these processes we will be informed and act accordingly. As Andrew McStay argues:

> To give consent is to act. Consent is not passive, but rather requires that people do something. This means that people must be informed and able to conceive an educated opinion so as to express will. Without this there is no consent, but rather the application of force. In expressing will there is agency, volition, control, deliberateness and making something happen. To be devoid of understanding is to be unable to give proper consent (McStay, 2013: 600).

As McStay highlights, without understanding what is happening to us in the online environment there is no consent, but rather – forcing us to participate. One of the problems is that we just do not have the capacities to understand what is happening in the backend. This is what Mark Andrejevic calls the *big data divide* which is created because "putting the data to use requires access to and control over costly technological infrastructures, expensive data sets, and the software, processing power, and expertise for analyzing them… The forms of 'knowing' associated with big data mining are available only to those with access to the machines, the databases, and the algorithms" (Andrejevic, 2014: 1676). Since most of us 'regular' people who use digital services and systems do not have these processing capacities, we simply cannot comprehend what can be done with the data extracted from our bodies and movements. In the next section I will outline the ways legal and design scholars have been debating 'consent', and especially what they have been

missing.

“Pro-choice” - Legal and design justifications of consent

In the USA, the first broad recognition of consent within a privacy framework was the 1973 Department of Health, Education, and Welfare (HEW) “Fair Information Practice Principles” (FIPPs) that were later adopted as part of The Privacy Act of 1974. In the European Union, Germany’s Federal Data Protection Act in 1977 and France’s data protection law from 1978 are considered to be the first iterations where consent is integrated within data processing laws. Later on, consent was introduced in the 1995 Data Protection Directive (95/46/EC) where it was defined as “any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed” (European Parliament, 1995). A few years later the definition of digital consent stayed the same in the e-Privacy Directive (2002/58/EC), which was a law that tried to regulate electronic communication. In 2018, the GDPR came into force and introduced new ways of operating consent, mainly requiring explicit consent through opt-in mechanisms which meant that inactivity or silence did not indicate consent. However, underlining this evolution is the fact that consent is about whether people agree to a specific communication *about* them, with data extracted from them, rather than communication *between* them, as the senders or receivers of messages (content). In other words, people became the message (data) and not the respondents of the digital/electronic communication.

As the paragraph above shows, consent was mentioned in various EU laws, however, it is only in 2011, that the Article 29 Working Party, an advisory body on data protection issues in the European Union, provided a clearer definition of what consent means. According to them it has to be: freely given; informed; explicit; specific; informed; and unambiguous. This was framed under the notion that people gain control, agency, self-determination and autonomy by pressing a button that says ‘agree’. What these definitions illustrate is how Western philosophy has influenced legal approaches to consent. They assume that with the right type of information, people will be informed and will have the freedom and control to express their autonomy by choosing the option that fits them.

According to this approach, we all have the power and, at the same time, the responsibility to learn what is happening to the data extracted from us. However, as Woodrow Hartzog argues, “[e]ven users who attempt to educate themselves about websites' privacy policies often do not fully understand the policies and the powers they give websites regarding the use of personal information” (Hartzog, 2010: 1647). As Hartzog identifies, contracts that websites and services offer people are meant to protect the websites, and not the users. In this way, asymmetric power relations are created, and consent operates as an enabling

mechanism to this new type of exploitative relationship.

Legal scholars have been debating what the meaning of consent is in the digital environment and its validity, for more than two decades, mainly in the context of privacy laws. Many scholars argue that the current legal system is problematic and insufficient for various reasons, such as the length of policies, the complex language, the inability to assess risk in these situations, and the limitations of real choice (Cate and Mayer-Schönberger, 2013; Acquisti et al., 2015; Borgesius, 2015). As Chris Hoofnagle argues, "whether consent is manifested through visiting a website or the millisecond action of clicking on a box, we know it is a contrived exercise" (Hoofnagle, 2018: 163). Adding to this, Solon Barocas and Helen Nissenbaum have said more explicitly that consent is a deception: "commonly perceived operational challenges have distracted from the ultimate inefficacy of consent as a matter of individual choice and the absurdity of believing that notice and consent can fully specify the terms of interaction between data collector and data subject" (Barocas and Nissenbaum, 2014: 45). So, what is consent for?

As Barocas and Nissenbaum argue, the discussions around consent are centered around the 'operational challenges'; legal scholars mainly debate which elements of the law should change to make privacy laws more effective and efficient. Daniel Solove (2012) calls this the 'consent dilemma', which is the problem of trying to find a version of consent that protects privacy but avoids paternalistic solutions which might limit people's choices even further. As Julie Cohen adds:

> Meaningful consent requires meaningful notice, but the information provided about data collection, processing, and use tends to be vague and general. Equally important, such disclosures tend to conflate important distinctions between remembering users' preferences, creating predictive profiles that may also include other, inferred data, using those preferences for target marketing, and tracking users across multiple websites, devices, and location (Cohen, 2019a: 4).

Along with issues around how consent should be applied to make sure people's rights can be protected, the bigger issue seems to be the huge difference between formal laws and how things are conducted in practice. As Alexandra Giannopoulou identifies, "there is a discrepancy between the formal requirements of the law and the practices observed in real life applications of data protection" (Giannopoulou, 2020: 4). In other words, many companies do not respect the laws that aim to protect people's rights, and at the same time, digital consent mechanisms act as legally binding contracts that force people to participate in this extractivist datafied ecosystem without understanding what it means.

Some of the solutions offered by legal scholars have been: to move away from framing this new relationship as a type of free transaction to an exchange of value which preserves consumer protections (Hoofnagle and Whittington, 2014), separates the notice from consent (Susser, 2019), and provides more transparency and alternative disclosures

(Bruening and Culnan, 2015). But these design solutions, along with the regulatory interventions such as GDPR, do not attend to the core issue of the exploitative business model and the deceptive ecosystem that enables it.[1]

Some of the design biases that are part of digital consent revolve around problematic interface design and default setting, what is often called 'dark patterns'. This can be whether the default setting of consent is opt-in or opt-out, or interface designs such as misleading wording, hiding away privacy-friendly choices, take-it-or-leave-it choices, pre-selected choices, or making privacy friendly options require more effort (Forbrukerrådet, 2018; Nouwens et al., 2020; Gray et al., 2021). Such design manipulations can constrain, restrict, nudge, shape, manage and construct how we behave on these digital spaces. As Ari Waldman (2018) argues, "our freedom is constrained by the design of the interface, the capacities of the server, and the platform's data use practices. And when we try to understand a website's privacy policy, we are similarly constrained by the way it is framed, presented, and designed" (Waldman, 2018: 99). As Waldman emphasizes, design configures people. When design serves and enables a specific business model, then any change made will still produce similar outcomes. Design also flattens experience into a singular option, disregarding people's levels of literacy which are influenced by their backgrounds, education, age, socio-economic status, physical and mental abilities and emotional state (Carmi et al., 2020).

The GDPR was supposed to provide citizens more power to object, contest and gain control over their personal data. For example, 'Article 21 - the Right to Object' is supposed to enable people to refuse the processing of their personal data, including common practices used by digital advertisers such as profiling. But how can you object to something when you do not understand how your data can be used to harm you? In order to object, people first need to know what data are, how they can be used and when, which companies are involved in this process, for how long people's data can be used and for what purposes and more. In the next section, I will show how key feminist concepts reveal how digital consent is flawed.

Feminist critique

In this section I present a feminist critique of the arguments outlined above about digital consent. I will focus on four feminist concepts to show that digital consent does not work for people but reproduces power asymmetries where people have no chance against technology companies. This critique is a larger critique of the way the online ecosystem is theorized and rationalized by legal and technical discourses, but specifically how consent has been used to authorize and legitimize exploitative and harmful practices to make the

[1] However, a few legal scholars recognise this, such as Julie Cohen (2019), Lilian Edwards (Edwards & Veale, 2017), Michael Veale (Veale, Binns & Ausloos, 2018), Seda Gürses (Gürses, Overdorf & Balsa, 2018), and Jef Ausloos (2020).

current business model work. Therefore, this critique is aimed at uncovering the systemic and institutional power asymmetries and how they harm people.

Feminist technoscience, cyberfeminists and posthuman feminists have been examining topics of the politics of knowledge production, science and technology, embodiment, digital spaces and information systems for decades. However, as the dominant discourses of science and law are still dominated by Western theories of epistemology and ontology, feminist approaches have remained in the fringes. In order to show how digital consent is flawed, I will demonstrate how four key feminist concepts - process, embodiment, context, and network - counter the dominant discourses about digital consent.

1. Process

Feminist technoscience scholars such as Donna Haraway (1988), Rosi Braidotti (2002) and Karen Barad (2003) have developed 'process-based' philosophies, each one in a different way. For example, Braidotti (2002) calls this 'becoming' while Barad (2003) calls this 'performativity' or 'agential realism'. Broadly speaking, they argue that different ontologies and epistemologies are not fixed but rather an ongoing process of being (co)produced. They reject fixity and essentialism and show the politics of the way different things come to matter. So instead of having clearly bounded boundaries of things like Western philosophy often argues, feminist technoscience show that processes of making a distinction between fundamental categories we know such as human, nonhuman, machine and animal are not as clear cut as we were led to believe.

Digital consent is usually prompted by a banner, pop up window or other features which require people to indicate if they agree or not to processing of 'their data'. The opportunity to express consent or rejection is presented at the beginning of the communication between people and different services and spaces. Consent is presented to us as a one-time indication of agreement or disagreement of procedures conducted on our bodies. But just like when consent is applied in sexual contexts, this is not a one-time expression, but an ongoing process of negotiation. I can say I want to have sex with someone at the beginning of a date and change my mind after two hours. Unlike sexual contexts, the type of communication, the architecture where it is happening in, the time of the 'event', and the actors involved are different. This is because, as I discussed above, I do not know who I am communicating with because *I am the message*.

The GDPR does provide EU citizens the ability to access (Article 15), object (Article 21), correct (Article 16) and erase (Article 17) their data, but these actions can only be initiated after the person has already started the 'communication' and their data has been extracted, stored, packaged and repackaged. Importantly, I do not know the dozens and hundreds of companies that are communicating 'me'. These actions require people to know and understand what is happening to them to begin with. It requires knowledge, time and resources, which might take months if not years before their local Data Protection

Authority will provide an answer. Portrayed as 'empowerment', these rights actually put the burden on people to challenge the default settings of the digital consent process. This new ecosystem produces two separate processes: one which is fast and easy-to-use interface designs to extract, sell and bid for our data, and the other offers laborious and complicated procedures as well as time and resources constrained to challenge them. This is how power imbalances are produced.

The problem is that we do not even know which part of us is being extracted and how it can be assembled and reassembled through other databases created by other data brokers. Therefore, demanding changes to our data becomes a challenging task when our sense of what this data entails is unclear. As Julie Cohen argues, "[s]elfhood is a process, not a state, and that process is discursive and social; it is informed by a sense of the self as viewed from the perspective of others. Interactions with automated logics disrupt processes of self-formation because the others whose perspective must be assimilated are so alien that their perspective cannot be imagined" (Cohen, 2019b: 10). Importantly, the temporal aspects of this communication process are unknown because it does not have a clear beginning and end.

Facebook, for example, was revealed as continuing to spy on people whether they had a subscription or not, whether they were logged into the platform or not, and whether or not people had asked to opt out of cookies. Facebook is not alone, many other companies send cookies that continue to communicate people's behaviors without their knowledge. As Johnny Ryan shows (2019), during real-time-bidding there is what he calls 'data leakage' which means that companies receive different data (us) during the bidding process even if they do not win the bid. That means that multiple companies continue to communicate data with different companies, and assemble a richer database of our profiles/segments. This goes far beyond the moment of arrival to a website or service and spans over an unknown amount of time during which we are traded continuously and within milliseconds.

In addition, as I show above, the definition of 'processing' entails around 17 different practices, some are conducted simultaneously but in different times. So, although digital consent is presented to us as a single 'event', it actually involves multiple events that are happening continuously with actors we are not aware of and for purposes we are not aware of, or can understand. What these practices show is that unlike the premise of digital consent, this is not a 'regular contract', we "are forced to take an oversimplified binary option between agree or disagree, while the latest ultimately means opting for some level of digital exclusion" (Peña and Varon, 2019: 13). It is an ongoing process whereby people are given only one chance to express agreement to processing activities that are happening continuously.

2. Embodiment

One of the big confusions around the online ecosystem and specifically digital consent is around the relationship between us and the data that is extracted from us through surveillance mechanisms such as web-cookies. Feminist technoscience scholars have always challenged rigid and fixed categories, especially of the body. As Karen Barad argues, "'[h]uman bodies' and 'human subjects' do not preexist as such; nor are they mere end products. 'Humans' are neither pure cause nor pure effect but part of the world in its open-ended becoming" (2003: 821). What she means is that there is no clear distinction between our biological bodies and computer simulation, or in our case data that is extracted from our behaviors, preferences and interactions.

Similarly, posthuman feminists like Katherine Hayles (1999) have been arguing that the human and posthuman are co-created and are always in the process of becoming. Coming from the field of literature, she has been arguing that there are no clear distinctions between science and science fiction and that both feed into each other and co-create one another. As she argues "[t]he posthuman subject is an amalgam, a collection of heterogeneous components, a material-informational entity whose boundaries undergo continuous construction and reconstruction" (Hayles, 1999: 3). A good example for this is that there is no clear distinction between 'being online' and 'being offline'. Even if I am drinking with friends at a pub, my phone is still connected to Twitter, Facebook, my email and other digital environments, I am never really 'offline'.

The current datafied ecosystem has augmented our bodies in ways we cannot comprehend. One of the greatest achievements of the surveillance capitalism project was the ability to distance people from their data and dehumanize it to make it seem separate from us. "Data is the new oil" is a slogan that has been promoted in various places such as the publisher Forbes (Bhageshpur, 2019) and government bodies such as the European Parliament (2020). The separation of humans from the data extracted from them is a necessary step to turn them into objects and then products. In this way, people do not fully understand that when governments and businesses talk about the economic potential of 'data', this means spying, measuring and trading them. As Koen Leurs argues, many big data discourses reflect positivism and disembodiment, however, "aggregate data is still connected to embodied experience, even though there is the claim that it is removed from identity and personal meaning-making" (Leurs, 2017: 132). Data are us, our stories and our contextual experiences – even if many times they do not accurately represent who we are, what we think and what we want – they are still part of us.

Setting commitments for feminist data studies, the Feminist Data Manifest-No scholars argue that they "refuse to understand data as disembodied and thereby dehumanized and departicularized. We commit to understanding data as always and variously attached to bodies; we vow to interrogate the biopolitical implications of data with a keen eye to gender, race, sexuality, class, disability, nationality, and other forms of embodied

difference" (Cifor et al., 2019). But while data are us, they are only part of us; We do not equal our data. Because when companies extract data from us, they take away the context it was performed in; it moves away from the history, culture, and social dynamics that made this behavior or preference meaningful to us (Lupton, 2020). And precisely this dehumanization and disembodiment make data portable, an exchangeable currency in the adtech ecosystem.

3. Contextual

The reduction of our human lives into data that can be moved and traded also involves taking data out of context. Because if data is out of context that means that it can be moved, used and applied in different contexts and importantly - traded between different companies for different purposes. Donna Haraway (1988) argues that feminist technoscience wants to reveal the biases in scientific truth claims which are universal and presented as objective. As she argues "[f]eminist objectivity is about limited location and situated knowledge, not about transcendence and splitting of subject and object. It allows us to become answerable for what we learn how to see" (Haraway, 1988: 583). Importantly, Haraway calls for situated, embodied knowledges and partial perspectives, while going against irresponsible knowledge claims, those that cannot be called into account.

Continuing Haraway's project, feminist data scholars Catherine D'Ignazio and Lauren Klein (2020) call this Big Dick Data, which are "big data projects that are characterized by masculinist, totalizing fantasies of world domination as enacted through data capture and analysis. Big Dick Data ignore context, fetishize size, and inflate their technical and scientific capabilities" (D'Ignazio and Klein, 2020:151). The surveillance adtech ecosystem relies on Big Dick Data, companies like Google and Facebook use different tracking mechanisms on a global scale to continuously track people on multiple digital platforms and services. They extract data to create and infer profiles and segments that are then traded in multiple places globally. Big Dick Data needs consent to disregard your contextual preferences.

While media scholars have been pointing out the complexities of context (Marwick and boyd, 2011) what they mainly talk about is the type of communication, i.e. content, conducted by people in various places, for example when people tweet and do not expect strangers to read or use that. However, when we talk about digital consent the discussion is around how pieces of us are being used in contexts that we do not know about. That could be taking some data about us from Facebook and then applying it in health insurance assessment conducted by our employers without our knowledge. So if you searched on Google's search engine for cancer, that information can then be used to assess what type of health insurance you should get, and if you might be considered as a health risk for a company and therefore should not be hired in the first place. This type of communication uses you as the message, but the communication is not *between* you and your employer, it

is between the insurance company, your employer and possibly several data brokers that have combined data *about* you that they thought would be relevant to them.

One of the main media law scholars to discuss this issue is Helen Nissenbaum (2004) who argues for 'contextual integrity'. As she argues, there are two types of informational norms: norms of appropriateness and norms of flow or distribution, and contextual integrity is maintained when both of the norms are being followed, and they are violated when one of them is not followed. Norms of appropriateness "dictate what information about persons is appropriate, or fitting, to reveal in a particular context" (Nissenbaum, 2004: 138) while norms of flow or distribution govern "movement, or transfer of information from one party to another or others" (Ibid: 140). When it comes to data brokers, however, Nissenbaum's analysis seems to be problematic, how can there even be contextual information norms when the multiple contexts we are applied in are unknown to us?

In a later account, Barocas and Nissenbaum argue about data that "because its value is not always recognized at collection time, it is difficult to predict how much it will travel, how much it will be in demand, and whether and how much it may be worth. In the language of contextual integrity, unless recipients and transmission principles are specified, the requirements of big data are for a blank check" (Barocas and Nissenbaum, 2014: 59). In other words, because we do not know which pieces of our data (us) companies use in multiple contexts, in multiple times and purposes we simply cannot know when informational flows are appropriate or maintain the norms of distribution. Context matters, but when the adtech ecosystem decontextualizes and dehumanizes us it becomes impossible to apply norms that are appropriate to us, and instead, norms are enforced on us.

4. Network

One of the reasons people in the European Union are required to give their consent to begin with is that there was an artificial line drawn between personal data and non-personal data. This division means that certain types of data are categorized as personal, and these are defined according to GDPR's Article 4(1):

> 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (European Parliament, 2016).

Feminists have long been arguing that the division between private (the personal) and public (not personal) was part of social constructions. The lines drawn between what are private and public spaces or bodies and what can be done in and on them, therefore, is highly political and influenced by social conventions. But while many feminists advocated

for an understanding that the "private is public" (MacKinnon, 1989: 191), what we see in the online space is more complex. As I argue elsewhere, the new business model that the digital advertising industry created "required that only specific spaces and activities that would be dedicated for direct financial transactions will be private, such as email and paying for online shopping. The rest of the spaces that will yield indirect revenue for funding the web through advertising will be public and, therefore, not private" (Carmi, 2020a: 136). This means that in the online ecosystem - everything is personal.

The situation in the online environment is different because the types of data that we produce overtly, or that are extracted from us covertly, leave multiple types of data points across multiple places from apps, to web and games. If we take our argument about embodiment to mean that different things that we do on mediated spaces are part of us, our bodies and identities, then even if these are specific pieces of us, they are still part of us, and hence identifiable and personal. Therefore, when cookies, pixels and other spying mechanisms are sent to be attached to our bodies and communicate our activities to entities we do not know, they understand who we are and, importantly - also our networks. As De Montjoye et al. (2015) show, people can be identified with very few data points. Other scholars like Paul Ohm (2009) have been arguing that we are never really anonymous and that true anonymization is not possible. Going back to the GDPR definition of 'personal' data I would argue that since just a few data points can identify a person that makes all of our activities personal because they can be linked to us. As journalist Shoshana Wodinsky (2021) argues:

> Any of these data points aren't necessarily going to be tied to me, Shoshana, because they don't have to be to make other people money. What this data is tied to might be something like my computer's unique IP address or my phone's mobile ad identifier, which are, on their own, anonymous. But even that particular data point isn't truly worth that much— advertisers, on a day-to-day basis, are looking at my data (and yours) as it's aggregated with data from an untold number of other people. A person's individual "data," on its own, is pretty much worthless; after all, marketers can't guarantee that I'll be clicking on a given ad or buying the product they're selling. What is valuable is when that data's in aggregate, even if it's "anonymized" and not tied to any one individual.

The Cambridge Analytica case from 2016 is a great example of how the datafied ecosystem provides corporations power through networks of people. The company managed to reach more people thanks to Facebook's API that enabled app developers to extract the data of people's friends. In addition, the company also used multiple datasets and combined them to create profiles. Whether or not the campaign was successful is beside the point, the key take-away from that case is that different data that are extracted from people's profiles and actions in various places are aggregated and analyzed, including their peers, family, colleagues and friends. In fact, many apps and games these days ask to get 'access' to your contacts, from LinkedIn, Facebook, Spotify and even Pokémon GO, and some of them even

ask you to 'Find Your Friends', which means you upload your contact list – your friends' 'personal data' – to an unknown database.

So pieces of you in various places may not mean anything in the particular context that they were expressed, but put together with other data aggregated from multiple places and corporations can gather or infer a profile on you, and from that produce similar audiences. Therefore, the artificial distinction between 'personal' and 'non-personal' data, is wrong and ignores the affordances of computational processes that spy, aggregate, combine and recombine *us and our networks* in endless ways and within a millisecond.

Educating for consent

Now that we understand that digital consent is flawed, the next question is what are the consequences of this on people? It is difficult to establish what the impact of digital consent is, because people's experiences vary according to their cultures, histories, socio-economic and education backgrounds, emotions, cognitive and body abilities. All these factors and more influence the way people understand, interpret and behave, and therefore it is impossible to isolate consent from people's experiences. But what we can do is show the accumulated effect on people; what this type of online ecosystem means in the broader sense. I will illustrate this through two main effects that show how consent limits what we do, think, understand and imagine: narrowing our agency; and surveillance realism.

In the first case, we can see that through the false narrative of control, people's agency has been narrowed. As Robert Gehl (2014) shows, this was an intentional strategy by the digital advertising industry who portrayed us as the 'sovereign interactive consumer' - a free and autonomous self-manager who has the power to be educated about the 'right' choices on the internet. According to this logic, we have the power to know and understand what is the business model, how companies extract us into data and then trade us and then we can, if we choose to, change the privacy setting and use the GDPR to change how our data has been used. However, as Gehl argues, if you decide you do not want to learn and educate yourself about these things this is considered as your fault, and the digital advertising industry will not help you.

In this way, as Lindsay Weinberg (2017) argues, the responsibility is placed on people to "perform autonomous self-management and cultivate the skills and literacy necessary for determining whether to engage with certain services and platforms" (Weinberg, 2017: 10). As Becky Kazansky argues, this kind of transferring the responsibility to people is known as 'responsiblization', and it encourages "an emphasis on the individual as the primary locus of responsibility for protection from harm… [and has] the convenient effect of deflecting attention from its causes" (Kazansky, 2015). In this way, digital consent is used as a mechanism that transfers data and hence profits to companies while shifting the responsibility of harm to the citizens and this is how the power asymmetries are drawn,

enacted and preserved. As I argue elsewhere, digital consent:

> naturalizes and normalizes digital advertising and technology companies' terms of use for their technologies and services. It teaches people the boundaries (actions and spaces) that they can operate in… It also marks the boundaries of what people can demand and expect from commercial actors and state regulators. This signals that what people could do on the web was not open for discussion, negotiations or multiple options (Carmi, 2020a: 161).

This leads us to the second effect: because people understand that their choices on the internet happen within the remit of the business model of surveillance capitalism it is hard for them to imagine the world without it. Digital consent helps cement this business model as the only way and overrides possible alternatives. It helps normalize surveillance and actively construct it as inevitable, what Lina Dencik (2018) calls *surveillance realism*. As she argues, it restricts and regulates the public's thoughts and actions. This means that people have come to accept and 'give up' or 'resign' (Draper and Turow, 2019) in trying to resist or create different narratives and realities in relation to surveillance, despite concerns and fears over the mass coercive collection and processing of their data. At the same time, people also consider surveillance as normal and start spying on their friends, romantic partners and employees in what is called 'social surveillance' (Marwick, 2012). Importantly, this normalization of surveillance has limited and prevented discussions of alternative ways of thinking about the online ecosystem.

Conclusion – refusing to consent

In this article I argue that digital consent is flawed. I show this by using four key feminist concepts – process, embodiment, context and network. I argue that the new adtech ecosystem introduced new kinds of communication systems where we are the 'message'. We are communicated between different companies that send various spying technologies to be attached to our bodies and continuously extract more data about what we do, where, when, and with whom. Instead of a one-time event, surveillance capitalism operates multiple procedures in an ongoing *process* with our *embodied* data by dehumanizing and de*contextualizing* us to package and repackage us in various *networks*. This paper does not intend to offer an easy solution or 'fix' this, but rather refuse to acknowledge that this works for us.

By doing so, I use what postcolonial feminists call 'refusal' to consent to the current situation. As Audra Simpson (2017) argues in relation to colonialism and the ruse of consent, settler governments forced indigenous people to sign treaties that were not signed under equal conditions. These agreements, as she says, meant that recognition was bound with consent and legally transferred rights to lands, resources and jurisdictions to settler governments. However, "'[r]efusal' rather than recognition is an option for producing and maintaining alternative structures of thought, politics and traditions away from and in

critical relationship to states" (Simpson, 2017: 19). But since today's big technology companies are bigger and more powerful than states, I choose refusal and apply it in the context of the exploitative surveillance adtech ecosystem they created and manage.

As I demonstrate in this article, although legal and design scholars agree that digital consent is problematic, they nevertheless reaffirm the current asymmetric power relations by offering 'solutions' that will try and make it work. These cosmetic changes do nothing to challenge the power imbalance and, if anything, harm people further in educating them to understand that their life is an inseparable part of surveillance realism. I refuse this type of thinking that pretends to empower people by providing them 'freedom of choice', because what is actually happening is narrowing, limiting and controlling people's agency, understanding, and imagination. I refuse easy answers to structural problems, and I invite you to join me in refusing to accept the current system.

References

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, *347*(6221), 509-514.

Ausloos, J. (2020). *The Right to Erasure in EU Data Protection Law: From Individual Rights to Effective Protection*. Oxford: Oxford University Press. https://doi.org/10.1093/oso/9780198847977.001.0001

Barad, K. (2003). Posthumanist performativity: Toward an understanding of how matter comes to matter. *Signs: Journal of Women in Culture and Society*, *28*(3), 801–831. https://doi.org/10.1086/345321

Barocas, S., & Nissenbaum, H. (2014). Big data's end run around anonymity and consent. *Privacy, big data, and the public good: Frameworks for engagement*, *1*, 44-75.

Beauchamp, T. L. (2011). Informed consent: its history, meaning, and present challenges. *Cambridge Quarterly of Healthcare Ethics, 20(4), 515-523*. https://doi.org/10.1017/S0963180111000259

Bhageshpur. K. (2019). Data Is The New Oil -- And That's A Good Thing. Forbes. https://www.forbes.com/sites/forbestechcouncil/2019/11/15/data-is-the-new-oil-and-thats-a-good-thing/.

Borgesius, F. Z. (2015). Informed consent: We can do better to defend privacy. *IEEE Security & Privacy*, *13*(2), 103-107. https://doi.org/10.1109/MSP.2015.34

Braidotti, R. (2002). *Metamorphoses: Towards a materialist theory of becoming*. Cambridge, UK: Polity Press.

Carmi, E. (2017). Regulating behaviours on the European Union internet, the case of spam versus cookies. *International Review of Law, Computers & Technology*, *31*(3), 289-307. https://doi.org/10.1080/13600869.2017.1304616

Carmi, E. (2020a). *Media Distortions: Understanding the Power Behind Spam, Noise, and Other Deviant Media*. Peter Lang International Academic Publishers.

Carmi, E. (2020b). Rhythmedia: A study of Facebook immune system. *Theory, Culture & Society*, *37*(5), 119-138. https://doi.org/10.14763/2020.2.1481

Carmi, E., Yates, S. J., Lockley, E., & Pawluczuk, A. (2020). Data citizenship: Rethinking data literacy in the age of disinformation, misinformation, and malinformation. *Internet Policy Review*, *9*(2), 1-22.

Christl, W., Kopp, K., & Riechert, P. U. (2017). Corporate surveillance in everyday life. *Cracked Labs*, 6. https://blog.fdik.org/2017-10/CrackedLabs_Christl_CorporateSurveillance.pdf.

Cifor, M., Garcia, P., Cowan, T.L., Rault, J., Sutherland, T., Chan, A., Rode, J., Hoffmann, A.L., Salehi, N., Nakamura, L. (2019). Feminist Data Manifest-No. https://www.manifestno.com/.

Cohen, J. E. (2019a). Turning Privacy Inside Out. *Theoretical Inquiries in Law*, 20(1), 1031.

Cohen, J. E. (2019b). *Between truth and power: The legal constructions of informational capitalism*. Oxford University Press.

De Montjoye, Y. A., Radaelli, L., & Singh, V. K. (2015). Unique in the shopping mall: On the reidentifiability of credit card metadata. *Science*, *347*(6221), 536-539.

Dencik, L. (2018). Surveillance realism and the politics of imagination: is there no alternative?. *Krisis: Journal for Contemporary Philosophy*, 2018(1), 31-43.

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

Edwards, L., & Veale, M. (2017). Slave to the algorithm: Why a right to an explanation is probably not the remedy you are looking for. Duke Law & Technology Review, *16*(1): 18-84.

European Commission. (1995). Directive 95/46/EC of the European Parliament and the council on the protection of individuals with regard to the processing of personal data and on the free movement of such data. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046.

European Parliament. (2016). 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 Directive 95/46/EC (General Data Protection Regulation). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL.

European Parliament. (2020). Is data the new oil? Competition issues in the digital economy. https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/646117/EPRS_BRI(2020)646117_EN.pdf.

Gehl, R. W. (2014). *Reverse Engineering Social Media*. Philadelphia, PA: Temple University Press.

Gürses, S., Overdorf, R., & Balsa, E. (2018). POTs: The revolution will not be optimized. *arXiv preprint arXiv:1806.02711*.

Haraway, D. (1988). Situated knowledges: The science question in feminism and the privilege of partial perspective. *Feminist studies*, *14*(3), 575-599. https://doi.org/10.2307/3178066

Haraway, D. J. (1985). *A manifesto for cyborgs: Science, technology, and socialist feminism in the 1980s* (pp. 173–204). San Francisco, CA: Center for Social Research and Education.

Hartzog, W. (2010). Website design as contract. *American University Law Review,* 60(6), 1635-1672.

Hayles, K. (1999). *How we became posthumans*. Chicago, IL: University of Chicago. https://doi.org/10.7208/chicago/9780226321394.001.0001

Hoofnagle, C. J., & Whittington, J. (2013). Free: accounting for the costs of the internet's most popular price. *UCLA Law Review*, 61(3), 606-671.

Hoofnagle, C. J. (2018). Designing for consent. *Journal of European Consumer and Market Law*, *7*(4), 162-171.

Kazansky, B. (2015). FCJ-195 privacy, responsibility, and human rights activism. *The Fibreculture Journal*, (26 2015: Entanglements–Activism and Technology).

Leurs, K. (2017). feminist data studies: using digital methods for ethical, reflexive and situated socio-cultural research. *Feminist Review*, *115*(1), 130-154. https://doi.org/10.1057/s41305-017-0043-1

Lyon, D. (2019). Surveillance capitalism, surveillance culture and data politics. *Data*

Politics: Worlds, Subjects, Rights. Abingdon: Routledge, 64-77. https://doi.org/10.4324/9781315167305-4

Lupton, D. (2020). 'Not the Real Me': Social Imaginaries of Personal Data Profiling. *Cultural Sociology*, 15(1), 3-21. https://doi.org/10.1177/1749975520939779

Marwick, A. (2012). The public domain: Surveillance in everyday life. *Surveillance & Society*, *9*(4), 378-393. https://doi.org/10.24908/ss.v9i4.4342

Marwick, A. E., & boyd, d. (2011). I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience. *New Media & Society*, *13*(1), 114-133. https://doi.org/10.1177/1461444810365313

McStay, A. (2013). I consent: An analysis of the Cookie Directive and its implications for UK behavioral advertising. *New Media & Society*, *15*(4), 596-611. https://doi.org/10.1177/1461444812458434

Nouwens, M., Liccardi, I., Veale, M., Karger, D., & Kagal, L. (2020, April). Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (pp. 1-13).

Ohm, P. (2009). Broken promises of privacy: Responding to the surprising failure of anonymization. *UCLA law Review*, 57(6), 1701-1778.

Papacharissi, Z. (2010). Privacy as a luxury commodity. *First Monday*, 15(8). https://doi.org/10.5210/fm.v15i8.3075

Peña, P. and Varon, J. (2019). Consent to our Data Bodies lessons from feminist theories to enforce data protection. *Coding Rights*. https://codingrights.org/docs/ConsentToOurDataBodies.pdf.

Ryan, J. (2019). New evidence to regulators: IAB documents reveal that it knew that real-time bidding would be "incompatible with consent under GDPR". *Brave*. https://brave.com/update-on-gdpr-complaint-rtb-ad-auctions/.

Solove, D. J. (2012). Introduction: Privacy self-management and the consent dilemma. *Harvard Law Review,* 126(7), 1880-1903.

Susser, D. (2019). Notice After Notice-and-Consent: Why Privacy Disclosures Are Valuable Even If Consent Frameworks Aren't. *Journal of Information Policy*, *9*, 148-173. https://doi.org/10.5325/jinfopoli.9.2019.0148

Tufekci, Z. (2018). Facebook's Surveillance Machine. *The New York Times*. https://www.nytimes.com/2018/03/19/opinion/facebook-cambridge-

analytica.html.

Turow, J. (2012). *The daily you: How the new advertising industry is defining your identity and your worth*. Yale University Press.

Veale, M., Binns, R., & Ausloos, J. (2018). When data protection by design and data subject rights clash. *International Data Privacy Law*, *8*(2), 105-123. https://doi.org/10.1093/idpl/ipy002

Waldman, A. E. (2018). Privacy, notice, and design. *Stanford Technology Law Review*, 21 (1), 74-127.

Weinberg, L. (2017). Rethinking privacy: A feminist approach to privacy rights after Snowden. *Westminster Papers in Communication and Culture*, *12*(3). https://doi.org/10.16997/wpcc.258

West, S. M. (2019). Data capitalism: Redefining the logics of surveillance and privacy. *Business & Society*, 58(1), 20-41. https://doi.org/10.1177/0007650317718185

Wodinsky, S. (2020). 'Anonymized' Data Is Meaningless Bullshit. *Gizmodo*. https://gizmodo.com/anonymized-data-is-meaningless-bullshit-1841429952

Zuboff, S. (2015). Big other: surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, *30*(1), 75-89. https://doi.org/10.1057/jit.2015.5