Data Governance Network
Anchored by IDFC Institute

November 2020

Working Paper 13

Informed Consent - Said Who? A Feminist Perspective on Principles of Consent in the Age of Embodied Data

Anja Kovacs and Tripti Jain

internet democracy project

Data Governance Network

The Data Governance Network is developing a multi-disciplinary community of researchers tackling India's next policy frontiers: data-enabled policymaking and the digital economy. At DGN, we work to cultivate and communicate research stemming from diverse viewpoints on market regulation, information privacy and digital rights. Our hope is to generate balanced and networked perspectives on data governance — thereby helping governments make smart policy choices which advance the empowerment and protection of individuals in today's data-rich environment.

About Us

The Internet Democracy Project works towards realising feminist visions of the digital in society, by exploring and addressing power imbalances in the areas of norms, governance and infrastructure in India and beyond.

Disclaimer and Terms of Use

The views and opinions expressed in this paper are those of the authors and do not necessarily represent those of the organisation.

Design

Cactus Communications

Suggested Citation:

Kovacs, A., Jain, T. (2020). Informed Consent - Said Who? A Feminist Perspective on Principles of Consent in the Age of Embodied Data. Data Governance Network Working Paper 13.

Supported by a grant from Omidyar Network

Abstract

While consent continues to be a crucial element of data protection regimes around the world, it has also been diagnosed with numerous weaknesses as a tool to promote and protect individuals' autonomy. In this paper, we set out to learn from feminist theory around consent in general and feminist applied thinking around sexual consent in particular how consent regimes in data protection can be strengthened. We argue that such a journey will be promising because of the close entanglements between our bodies and our data. We particularly foreground feminist criticisms of the concept of "property in the person" to understand in more detail the profound harms that current data practices do to our personhood, as well as the ways in which consent is currently deployed to enable and even legitimise such practices, rather than challenge or reject them. Through close engagement with feminist thinking around consent, we then develop a list of feminist principles that will need to be followed if consent is to ever be meaningful in data governance. Finally, we outline three areas of change that the application of these principles immediately points to: changes related to the collection of data; changes related to the uses of data; and changes required to protect people who are especially vulnerable in particular. Making these shifts, we argue, is essential if we are to put into place a data infrastructure that is actually empowering for, rather than exploitative of people.

Table of Contents

Introduction

In current data protection regimes around the world, consent remains one of the central mechanisms around which user rights are operationalised. At the same time, however, and despite this centrality, criticisms of consent regimes are on the rise. Notices are too lengthy and hard to decipher by non-lawyers. Consent fatigue means that users simply tick the box, without inquiring into what they are agreeing to. And within a networked environment, is the kind of autonomy that consent aims to enable even possible anymore at all?

Is it perhaps time to move away from consent altogether?

While that suggestion has indeed been made (Matthan, 2017), in this paper we want to propose a different approach. Our starting point is a reconceptualisation of the nature of data itself, one which recognises the need to centre bodies in debates on data governance. In dominant conceptual and metaphorical understandings, data today is constructed as a resource that is simply out there, up for grabs and ready to be mined (Kovacs & Ranganathan, 2019). But such constructions are not well aligned with many people's experiences. Every time we feel uncomfortable sharing data, we are reminded that this data has direct actual or potential relevance to our dignity, autonomy, and even bodily integrity. In fact, as van der Ploeg (2012) has argued, with even the most intimate aspects of our lives becoming subject to datafication, the distinction between our physical bodies and our data bodies is becoming increasingly irrelevant. Our bodies and data are in fact deeply connected.

Recognising this connection opens up radically new ways of thinking about consent in data governance. As we will examine in this paper, ever since the theories of philosophers such as Locke, Hobbes and Rousseau came to constitute the underpinnings of the modern state, the notion of consent has arguably been at the heart of the legitimacy of modern institutions as well as central to the protection of the individual's bodily integrity, autonomy and dignity. Feminists in particular, however, have long critiqued liberal notions of consent, which presume agreement between individuals “free and equal”. Feminists have unearthed that power relations construct some of us as free and equal, and others as less so, making the latter's consent irrelevant or even impossible. They have also shown how this inequality structures the core institutions of modern life, whether they be political, social or economic.

Of particular relevance to the debate on data governance in this context are feminist critiques of the notion of “property in the person”, a central fiction enabling consent in liberalism. As we will examine in detail, such critiques focus in particular on the ways in which the markets in persons, made possible by this fiction, undercut subjectivity, through the establishment of relations of subordination.

An especially fruitful area for us to analyse the implications of the deployment of “property in the person” in practice, and feminist critiques of it, is that of sexual consent. Not only have feminist debates around sexual consent over the past four decades been extremely rich, in addition close connections have been established there, too, between bodies and subjectivity (see e.g. du Toit 2007; Lacey, 1998; Phillips 2013). Moreover, feminists working on sexual consent have put considerable thought into what needs to shift, in these circumstances, if consent is at all to become meaningful for all.

If we are to strengthen consent regimes in data protection, valuable lessons can, then, be learned from these existing debates about the form and direction such strengthening should take. Thus, through an examination of commonalities and differences between these feminist conceptualisations of consent and those in data protection frameworks, we will develop in this paper a list of core principles that can

guide a reexamination of consent in data protection. These guidelines should help policy makers and technology designers to ensure that consent is actually free, autonomous and meaningful at a time when data and bodies are increasingly entangled.

To achieve this, we will, in section two, briefly go into the history of the consent regime in data protection, and examine how consent is constructed and operationalised in dominant approaches to data governance. We will then outline what the weaknesses of current consent regimes in data protection are, as put forward in existing literature. In section three, we will move on to examine feminist perspectives on consent, in particular in the context of sexual relations. What are the salient characteristics of meaningful consent that feminist debates around sexual consent have highlighted? Finally, in section four, we examine how these findings from feminist research can help us to rethink consent in data protection, both at the individual and at the structural level. As our starting point is that data is embodied, it is essential, however, for the reader to get deeper insight at the outset into what this entails, and why we believe this reconceptualisation of data is so important. We will therefore start this paper with an elucidation of that approach in the next section.

1. Consent, Contract and the Datafied Body

1.1 Consent and Contract

To fully appreciate the importance and value of consent, as well as understand its limitations, it is essential to start from an examination of its central role in modern life. The notion of consent is at the heart of the liberal political philosophies, as well as institutions, that underlie and have shaped modern democratic societies. The social contract theories of Locke, Hobbes, Rousseau that form the basis of liberalism - and, more recently, of Rawls and others - take as their starting point that we are all born as free and equal individuals. If we are free and equal, how can the exercise of authority over us possibly be justified? According to social contract theory, and to liberalism, the answer lies in consent: for a relationship of authority and obligation to be legitimate, it is essential that we have voluntarily committed ourselves to it, i.e. that we have consented to it (Pateman, 1988).

Such constructions have, however, come under strong critique from, among others, feminist thinkers. The influential work of Carole Pateman (1988, 1989) in particular, has revealed that all too often, consent is merely a theoretical fiction, its existence assumed, asserted. In practice, a multitude of individuals and groups are never capable of consenting, and thus of participating fully in the political order. For example, with the exception of Hobbes, Pateman (1988) showed, both the classic contract theorists and later ones considered the subjection of wives to their husbands “natural”, thus effectively excluding women from the status of “free and equal individual” that is central to contract theory. Women's consent, then, became irrelevant. And while it might appear as if things have radically changed today, that marriage can now be a partnership based purely on the consent of two individuals, the continued legality in India of, for example, marital rape illustrates that that is not actually the case. The law continues to inscribe the assumption that rather than free and equal, women are naturally subjected to their husbands.

What Pateman and others have thus squarely brought out in their analyses is the importance of power relations in shaping “consent”. If liberal theory casts the legitimacy of our societies' institutions as the result of a shared worldview and values, this is only possible because it leaves out of its purview the

social circumstances under which different people give “consent”, with many left with little choice. In doing so, contract theory and its deployment of consent enable the recasting of subordination as freedom, while the operation of power disappears from view (Ackerly, 2008). Contract, thus, “becomes a modern mechanism for subordination” (Richardson, 2010, p. 58). The legitimacy of our social institutions is the result of the exercise of not freedom, as we have been made to believe, but of power (Ackerly, 2008).

1.2 Contract and Property in the Person

When assessing consent, not all contracts deserve equal attention, however. The contracts that should be of particular concern to us, notes Pateman (1988), are those that involve the concept of “property in the person”, as these are central to the establishment of relations of subordination. As Locke (1988) stated perhaps most famously: “every Man has a *Property* in his own *Person.* This no Body has any Right to but himself” (II, §27, emphasis in original). Thus, human beings are treated in contract theory “as if they were the owners of their abilities and attributes, viewed as 'property', which could be treated as if they were alienable” (Richardson, 2010, p. 56). The employment contract under capitalism, for example, is based on this assumption: that our skills and talents can be alienated in much the same way that material goods can. And because property in the person is considered “alienable it can be subject to contract” (Pateman, 2002, p. 21).

Pateman's work has established, however, that property in the person is in fact a political fiction (1988, 2002). Although our powers, talents, skills, capacities and abilities may be treated as separable from us, in practice, of course, they are not. In an employment contract, for example, we might only promise to provide our employer with our labour, skills and capacities, but these cannot be put to work without the whole of us being involved. The rest of our person cannot go off and do something else. In fact, Pateman argues (1988), the fiction of property in the person has become central to contrasting, for example, a slave with a wage labourer while hiding from view that the whole of the person is actually engaged in both cases. In modernity, a new type of relationship of subordination has, thus, been created through the device of the contract: one that is made to appear like an exchange, while *de facto* undermining the autonomy and right to self-government of the individual. Consent gives this contract its veneer of legitimacy.

1.3 From Data as a Resource to Data as Embodied

Pateman's arguments have renewed relevance in the context of debates on the governance of data that relates to a person, both where consent is concerned and more broadly. In order to understand why and how, it is essential to probe deeper into the nature of such data.

Dominant conceptual and metaphorical understandings of data today construct data as a resource that is simply “out there”, and therefore “up for grabs”, ready to be mined. These understandings of data as a resource find their roots in the development of the discipline of cybernetics, from the 1940s onwards, in which information came to be put forward as a layer which informs everything, yet which somehow exists independently from the medium carrying it, and so can be easily transferred from one medium to another (Hayles, 1999).

A radical manifestation of this understanding of data as disembodied can be found in the dream of scientists, such as Hans Moravec, to one day download human consciousness into a computer; the assumption here is that the body in which this consciousness presently sits is irrelevant (see Hayles,

1999). But this construction of data has had wide influence. For example, it is at the heart of the Karnataka Government's decision to require that individuals who have tested positive for COVID19 send hourly selfies with GPS coordinates to officials while under home quarantaine, using the Quarantine Watch app. While many would find it unacceptable to have an official visiting their residence on an hourly basis to investigate whether they are obeying quarantine orders, digital intermediation somehow makes such invasive monitoring acceptable (Ranjit, 2020). Moreover, in addition to facilitating greater state surveillance, the construction of data as dematerialised and disembodied also gives it its tremendous potential for economic exploitation, as we will explore in greater detail later in this paper. After all, if data is not really us, if it is at best a resource *about* us, we need not have any qualms about bringing it under market logic and making it subject to contract.

But understandings of data as dematerialised and disembodied sit uneasy with our experiences. As more and more decisions that affect our physical bodies are taken on the basis of our data bodies, we do not experience data as a disembodied reflection of our bodies, or as a layer that exists independently of it. In what arguably amounts to a fundamental reconceptualisation of our bodies (van der Ploeg, 2012), we increasingly experience it as an extension of our bodies, and even an integral part. Indeed, as van der Ploeg (2012) has argued, with the datafication of even the most intimate aspects of our lives, a fundamental shift is taking place: the distinction between our physical bodies and virtual bodies is, in fact, becoming irrelevant.

This is evident, for example, when victims of the non-consensual sharing of sexual images describe their experience in terms of sexual assault, not in terms of a data protection violation (Patella-Rey, 2018) - even if the latter is how laws around the world currently address it, if at all. Similarly, when people infected with COVID19 share their location and other data with the state through quarantine apps, they are conscious that the state's goal is not merely to access their data, but to ensure that their bodies remain confined to their homes (Ranjit, 2020). And aspects of their practices indicate that technology companies, too, recognise these fundamental connections between our bodies and data, even if implicitly: while they may continue to treat data as a commodity when analysing, trading and monetising it, it is after all only because of these connections to our person that such processes gain economic value (Mandel, 2017). If we are at times feeling uncomfortable when ticking a consent box, it is because at those moments, we are viscerally experiencing this fundamental shift in our own lives.

1.4 Embodied Data and Property in the Person

For the debate on consent in data protection, this reconceptualisation of data – grounding it not merely in metaphor, or in semiotics, but in people's material realities and experiences – has important consequences. Despite criticisms, proposals to move beyond consent – to instead focus, for example, on the accountability of data controllers (Matthan, 2017) – make perfect sense in a world in which data is approached as a resource. But when people and their bodies, both physical and virtual, are put back into the picture, questions of consent emerge centre-stage in data protection debates once again.

Pateman's critique of the deployment of property in the person in modernity is instructive in concretely thinking through what is at stake. When data is constructed as a resource, it is at best seen as alienable property in the person; proposals to compensate individuals for data they share with companies, for example, reflect such an understanding. But some data need not even be considered such alienable property. Data about a person that is inferred by a company about that individual on the basis of data that this individual has provided, for example, is generally considered property of that company, and not of the individual whom it concerns.

What treating data as a resource in this way hides from view, however, is that in the process fundamentally new relations of subordination are established. Yet, the intense datafication of our bodies, behaviours, emotions and lives is already under increasing criticism for doing precisely that. In her critique of surveillance capitalism, Zuboff (2019), for example, has argued that this new stage of capitalism is fundamentally geared to modifying our behaviour in line with the ends of others, or to automate us. As a consequence, its dynamics are severely eroding our space for individual self-determination as well as, for that matter, for social debate and democratic decision-making. Couldry and Mejias (2019), too, have critically commented on how allowing oneself to continuously be tracked has become a necessity of everyday life. They have noted that "the *very fact* of data collection through surveillance does [violence] to the minimal integrity of the self" (p. 156, emphasis in original), the minimal boundedness without which the self does not exist, as this space is "continuously invaded and subjected to extraction by external power" (p. 157).

If the manipulation of our data has had such an invasive and far-reaching impact on our personhood without this causing more of an outcry, the construction of data as a resource is not the only factor responsible for this, however. This has further been facilitated precisely by the digital nature of data and the simultaneous erasure of its material basis in and/or effect on our bodies and their actions. Because its digital nature allows data to be alienated, those who control the infrastructure to do so now can exploit and manipulate us at a remove, rather than having to commandeer us in person. In other words, data's digitality makes it easier for this centrality of our bodies, of the material world, to be obscured. Moreover, the processes through which this happens, as well as the amount of data they sweep up, can also remain opaque, or even unknown to many impacted, as they are at a distance. This makes mounting an effective resistance both more complex and less likely.

Data is, thus, a unique form of property in the person in that it is at the same time alienable, because of its digital nature, and yet central to the creation of fundamentally new relations of subordination today. Only when the connections between our bodies and data are reestablished does it become obvious that the fiction of property in the person today once again is enabling, legitimising and reifying deep inequalities and subordination. The question we seek to explore in the rest of this paper is the following: can consent fundamentally prevent such hollowing out of our autonomy, and if so, what conditions need to be fulfilled for it to be able to do so? Seeing that questions of consent and the body have figured extensively in feminist debates relating to agency, autonomy and dignity in sexual relations in particular, these provide a valuable ground to gain insight into possible answers to these questions. To begin this examination, however, we will start by exploring the historical evolution of consent in data protection regimes, so as to understand how we got where we are today.

2. Consent and Data Protection As We Know It

2.1 Consent and Data Protection, Then and Now

The concept of privacy in terms of technology first came to fore in the late 1970s. The growing prominence of this concept was a result of deliberations in the global north over fair information practices of legislative and investigative authorities with respect to collection and use of personal data of individuals through computerised processing (see "Annexure" to OECD Council, 1980).

In order to address these concerns, the Organisation for Economic Cooperation and Development

(OECD) set up an expert group for the years 1978-1980, under the chairmanship of Australian expert Michael Kirby, with the objective of drafting international principles for the protection of privacy. The expert group came up with eight privacy principles that later became the basic framework for the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD Council, 1980), adopted in 1985. Additionally, in 1981, the Council of Europe's binding convention for the protection of individuals with regard to automatic processing of personal data (Convention 108, 1981) was adopted. The convention has striking semblance with the OECD principles.

The principles aim to protect and safeguard the fundamental values of privacy, individual liberties and the global free flow of information. At the heart of the principles lies the basic tenet of collection limitation. According to it, the data collectors/processors can collect or process data under two conditions only, namely: 1) collection and processing for purposes deemed lawful by the nation, in cases where, due to a power asymmetry, it is not possible to seek meaningful consent; and 2) when the informed consent of the individual has been obtained for the purpose of personal data collection and processing.

Over the years, the condition for collection limitation, i.e. consent, has come to be seen as a means to regulate intensified intrusion into personal information of individuals. It is now widely avered that consent empowers individuals with the ability to control access to information about themselves, and to prevent it from being misappropriated by state and non-state actors. Whether the California Consumer Privacy Act, the EU's General Data Protection Regime (GDPR), India's draft Personal Data Protection Bill 2019, or the privacy policies of any technology company, specially those that provide services or products online, most of them prescribe for a “consent” regime.

However, over the last thirty years, with the evolution of technology, the consent framework has also come under growing criticism. Scholars (Matthan, 2017; Solove 2013) have pointed out that while data processing abilities have transformed, the consent model has remained static. This has important consequences. In the 1970s and 1980s, policymakers were primarily worried about legislative and investigative practices concerning the protection of privacy with respect to the collection and use of personal data recorded on physical databases such as CD-roms, individual computers, and floppy disks. With the arrival of the commercial Internet in the 1990s, however, systems of data collection and processing changed drastically: today, our personal data is also collected online, and in different ways, such as while browsing a web page or using an app; databases that store data are interconnected and often exist in the cloud; and, even small data storage devices have been replaced by large online and offline databases (Solove, 2004). Thus, with significant advancements in technology, the capacity to interconnect, analyse, identify, and extract new and unanticipated value from even odd or seemingly worthless data has progressed manyfold.

For example, Axicom Corporation, a consumer data analytics company based in the United States, has more than 23,000 computer servers collecting, collating and analysing data. The company reportedly performs over 50 trillion data transactions per year. Company executives have stated that its database accommodates information of about 500 million active consumers worldwide, with about 1,500 data points per person. Integrating everything that it knows about our offline, online and even mobile selves, Axicom creates in-depth behavioral portraits in pixelated detail. Its executives have called this approach a “360-degree view” of consumers (Singer, 2012).

It is not just the technology with respect to the collection and processing of data that has changed; the way data is perceived has undergone a tectonic shift as well. Earlier, personal data was perceived simply as information about individuals. However, today, data is not merely seen as information about others. It has become an asset, because of the high returns it can yield while the capital cost of collecting and

processing data remains relatively low. In addition, unlike other assets, data never gets exhausted (MIT Technology Review Insights, 2016). Reflecting on these dominant understandings of data, Brynjolfsson and McAfee (quoted in MIT Technology Review Insights, 2016) have remarked: "more and more important assets in the economy are composed of bits instead of atoms today".

2.2 The Weaknesses of Consent in Data Governance

As discussed earlier, most governance frameworks, such as the GDPR and the California Consumer Privacy Act, recognise that consent enables privacy self-management (Solove, 2013), and has normative value in ensuring autonomy. However, scholars (Cohen, 2019; Solove, 2013) have noted that consent is not a silver bullet and that the entire privacy regime cannot seek refuge in consent.

Researchers have argued that the current mechanisms to seek consent are inadequate and problematic in a number of ways (Acquisti et al., 2013; Goffman, 1959; Solove, 2013): from cognitive or perception problems to meaningful consent, to systemic or structural problems that the individuals can do little to address right now (Solove, 2013). In particular, the following have been highlighted in existing literature:

- **Inadequate notices**

In order to seek meaningful consent from individuals, it is imperative to serve them with adequate notices. However, at present, most privacy policies are long, full of legalese and difficult to understand. In fact, a survey conducted in India by Bailey et al. (2018) found that the privacy policies of companies such as Uber, Flipkart and WhatsApp are so complex that they can only be comprehended by individuals with graduate level reading abilities. As a result of this complexity, people do not read notices regularly, even if they do share their personal data to access these services (Nissenbaum, 2009). Such challenges are further compounded by the fact that these policies are also subject to future changes (Joint Committee on Human Rights, 2019).

It is also important to note that the harms from privacy violations are often not made tangible or obvious in such policies - in stark comparison to, for example, warnings regarding the harms of drinking while driving or smoking cigarettes. Since notices do not clearly demarcate the possible impact and risks in simple language, they generally are not very useful for individuals in decision making. Unless risks are made explicit, most individuals understandably cannot assess risks objectively, simply because they do not have sufficient knowledge or understanding of all possible outcomes of a privacy violation (Solove, 2013).

Thus, there is a clear disconnect between the expectations and reality of the notice and consent regime. Current data governance frameworks expect notices to enable individuals to make informed decisions. However, due to inadequacy of notices, individuals fail to understand the implications of the privacy policies, and are not in a position to furnish meaningful consent.

- **Consent Fatigue**

The consent regime not only suffers from inadequate notices, it is also affected by the number of times consent is asked for. Data protection regimes require individuals to read through lengthy privacy policies and manage consent for every application, service portal and website that they browse, access or use (Custers et al., 2014). These are extremely high expectations and an exercise that leaves individuals exhausted and frequently causes them to disengage.

Jolls and Sunstein (2005) also note that when people get accustomed to certain notifications, they learn to be oblivious towards them. This implies that overload of consent forms often discourages individuals from managing their privacy, which in turn would demean the intent of the consent regime (Custers et al., 2019).

- **Consent and adhesion contracts**

An additional challenge to meaningful consent is that at present, the contracts under which consent is being sought are mostly adhesion contracts: they require an individual to "agree" to a bundled set of terms of service to access a service (Davis, 2007). Such contracts do not provide a means to negotiate the terms of consent, or alternative means to access services or products online in cases where individuals are not willing to provide consent (Custers et al., 2014).

Not only are these contracts non-negotiable, most technology companies employ a set of standard contractual clauses to seek consent for different purposes and services. These standard contractual clauses have proven to be insufficient to seek meaningful consent because where the services accessed are different, there is no justification why the conditions of access should be the same. For example, why does an app that enables flashlight on a phone need location data or contact information?

From the above, it is clear that consent obtained on the basis of these non-negotiable standard privacy policies cannot be considered as "freely given". In fact, such policies dilute the notion of individual's autonomy, as a core principle of consent is that the individual should be able to negotiate or bargain (Bailey et al., 2018).

- **Data sharing arrangements with third parties are often not explicitly mentioned**

Consent of individuals is obtained on the basis of consent forms made available by applications or data controllers that are providing services or products to these individuals. However, in many cases, that data can then be processed and analysed by companies other than the one that seeks consent. It has been observed (Okoyomon et al., 2019) that 75% of mobile based applications deploy third party data processors for the processing of data. Of these, only 22% disclose the names of these third party processors and 10% fail to even mention in their policies that third parties will have access to the data, leaving individuals with no means to make informed decisions. Even if the policies disclose the names of or information about third parties collecting data, to know more about data collection the burden is on the user to read the policies of both: the host website or app, and the third party. This is an unreasonable expectation from the user in the existing privacy regime: estimates suggest that the average time required for a user to read policies of host and third party websites exceeds 84 minutes (Libert, 2018).

Moreover, most privacy policies include a saving clause along the lines of: "we are not responsible or liable for the privacy policies or practices of third parties" (Okoyomon et al., 2019). While most mobile applications use third parties for data processing, the apps cannot be held accountable for misconduct by these parties.

This opaque practice of not disclosing that third parties are being deployed circumvents an individual's right to informed consent. In fact, the assent obtained from individuals on the basis of such deceptive notices should not be considered consent as, left in the dark, the individual in such a situation cannot exercise their rationality. Rather, the assent obtained through such notices could be termed manipulation or coercion.

- **Impact of aggregation is hard to anticipate for individual users**

If the information about third party data sharing is made more explicit when consent is being sought, individuals will be better equipped to self manage their privacy. That being said, the disclosure of third party data sharing practices alone will not be sufficient in the world of businesses that thrive on big data, as such businesses collect and process massive amounts of data from innumerable sources on the Internet. Even aware and informed individuals who share their personal information on different occasions in isolation cannot anticipate the impact of this aggregation of data (Solove, 2004).

Take, for example, a woman who uses a fitbit: the fitbit maintains a record of her daily physical activities, including her sleep patterns, the number of steps she walks and her heartbeat patterns. In addition, her geolocation data indicates where she conducts her workouts, and her food delivery application data records what she eats. All this data will have been shared by her in isolated instances, but many technology companies, including Google and Facebook, aggregate all these data points, develop an individual's profile and sell it to companies that might target advertisements or design insurance policies for that woman or women with a profile similar to hers.

- **Users are unaware of the business models of data fiduciaries**

As Zuboff (2019) has argued, the reason that current notices fail to inform users is because users believe they are exchanging their data for a product or service and to aid the provisioner in improving that product or service - but increasingly, that is not what is actually happening. In the name of "personalisation", excess data is collected from users because that data, and the predictions that can be based on it about our future behaviour, are the ultimate goal of such exchanges. Data we may have provided ourselves or data that they derive regarding our habits, moods, experiences and thoughts while using their product or service is used by these entities to create profit-generating predictions regarding our future behaviour as well as, increasingly, to influence that behaviour in real time. Users are merely the raw material, and the provision of the product or service an occasion to get access to that material.

Since the growth of an increasing number of businesses today, from car manufacturers to toy makers, is entrenched in the data they collect, these businesses do not design technologies or provide terms of service that account for privacy. Instead, they invest in designing technologies and drafting policies that allow for maximising the extraction of personal data from users. This intent prevents businesses from explicitly informing individuals in their privacy policies about the risks and harms that may be inflicted upon them when they share their data (National Telecommunications and Information Administration, 2010), rendering individuals uninformed.

- **Consent is perceived in an individualistic manner**

An individual's own decision is not always sufficient to maintain control over their personal information in an extensively networked environment such as the Internet today (Marwick & boyd, 2014). Even if an individual personally refrains from giving consent to a platform or website, when their friends and family nevertheless share information about them, the chances are that the platform will still process the data that is made available by other parties about this individual (Quodling, 2018).

Consider, for example, a situation in which a person consents to being part of a social networking platform and also chooses to express her sexual orientation, while her friend abstains from signing on to the social networking platform (Pearson, 2014). If the person who is on the social media platform

uploads a picture of both of them, it is very easy for the platform to predict the sexual orientation of the friend who is not present on the platform through a simple statistical regression method (Jernigan & Mistree, 2009). The prediction is probabilistic and so might not be accurate; however, the more information the platform manages to glean about the individual, the higher the accuracy of prediction will be. Indeed, Hermstrüwer (2017) found in his study that with an increase in the personal data shared by one user, there is a significant increase in information and predictability about others, immaterial of their consent. This implies that seeking consent through individualistic notices is inefficient for such extensive networked environments. Not just that, the individualist approach to consent imposes negative privacy externalities on the other individuals (MacCarthy, 2011). This means that even if one individual exercises their right to privacy and does not share their personal information, if others have shared sufficient personal information about them, the damage is still done.

Since the current consent regime fails to acknowledge that the concept of privacy is inherently social in these networked environments, consent obtained according to existing methods that perceive consent as individualistic is meaningless. In fact, this regime leaves individuals in a constant social dilemma: whether to give consent or not when their personal information is mixed with the personal information of others (Fairfield and Engel, 2015; Regan, 1995).

- **Consent regime is static while modes of data collection and business models have changed**

With the advancement of technology, the modes of data collection and appropriation have also transformed. New tools, such as facial recognition and facial detection, have emerged. For example, facial detection enabled billboards can determine age, gender and moods, to queue advertisements instantly for their viewers (Article 29 Data Protection Working Party, 2012). Challenges arise when traditional methods of consent are deployed with regard to such technologies. As these billboards are installed in public spaces such as grocery stores, shopping plazas and parking lots, consent forms or privacy policies cannot be distributed to seek informed consent from every passerby or bystander.

Most companies that have designed and deployed facial detection billboards, such as Quividi (2019), claim that the billboards do not record personally identifiable data and that data is recorded for very short periods, i.e. only for the time an individual is looking at the billboard (Smith, 2018). For these reasons, the companies deploying these facial detection billboards argue, they do not need to seek consent while obtaining data from bystanders or bypassers. However, while the data collection and processing by such billboards may currently not pass the threshold of identifiability that requires that a person can be "distinguished" within a group of persons on the basis of that data, that data does indisputably concern a specific individual (Davis, 2020).

Moreover, the technology deployed by billboards has the ability to categorise individuals and serve advertisements on the basis of stereotypes. For example, the billboard may serve adverts for skin-lightening products only to people with darker skin, thus not merely stereotyping individuals but also reproducing problematic social norms of desirability relating to skin colour.

Lastly, currently these pervasive technologies are mostly used to advertise products. However, there are companies that have heavily invested in and are trying systems that assess suitability of a candidate for a job, detect lies, and diagnose disorders, among others, on the basis of facial recognition (Heaven, 2020).

In each of these cases, it deserves greater consideration what the possible harms of such data collection and processing are, whether they should be allowed in the first place, and what role consent could play in managing related risks, if at all.

What deserves to be highlighted here is that common to all these weaknesses of current consent regimes is the construction of data as a resource. Not altogether different from any material resource that can be traded, this construction has made it possible for data to be reduced to merely a means of exchange, enabled in contract by consent. If data-driven entities are able to engage with impunity in the appropriation of our data, both with depth and breadth, as described by Zuboff (2019), the portrayal of our data as a fair consideration for the services or products that these companies (and, increasingly, governments) supposedly provide to individual users has been essential.

The understanding of data as a resource is not limited to non-state actors; it is also reflected, for example, in the EU Proposal for a Directive on certain aspects concerning contracts for the supply of digital content (Directorate-General for Justice and Consumers, 2015). The proposal recognises data as primary means to "pay" the online service provider instead of money, and consent as a means to facilitate this transaction. Thus, personal data is perceived as a valid consideration for exchange of services, and consent forms are treated as mere contracts governing that exchange. Through the mechanism of consent, the data relations of subordination that are established in the process are legitimised.

3. Feminist Perspectives on Consent

When consent seems to fail in so many ways, does it make sense to pursue the strengthening of consent mechanisms nevertheless? Can consent be rescued from this quagmire?

Putting bodies back into the data debate points to the urgency of revisiting that question in depth. As Troost (2008, p. 171) has pointed out, "though the form and intensity may vary, any oppression you care to name works at least in part by controlling or claiming ownership of the bodies of those oppressed". Within feminist debates relating to agency, autonomy and dignity, one area in which questions of consent and the body have, thus, been subject to particularly rich discussion is that of sexual consent.

In order to understand the potential meaning, value and role of consent in the age of datafied bodies, an exploration of consent in these feminist debates therefore provides a valuable starting point for answering that earlier question, as well as to gain insight in what needs to change for consent in data governance to become more meaningful.[1] It is to this exploration that we turn our attention in this section.

3.1 Feminists Debate Sexual Consent

Since at least the 1990s now, the notion of consent has been at the forefront of feminist campaigns against sexual violence (Loick, 2019). Liberal feminists, in particular, have tried to use the notion of consent to expand women's choices and strengthen their agency and freedom as individuals. They have done so by fighting for the criminalisation of all forms of non-consensual interactions, or assaults, as

[1]Peña & Varon (2019) also propose we learn from feminist debates around consent to build more meaningful consent in data governance, and there are many overlaps between the feminist principles for consent they delineate and the ones that we outline later in this paper. However, the premises on which their study is built are very different from ours. To ensure that our proposals are firmly rooted in a recognition of the entanglement of data and bodies, we therefore systematically examine similar ground once again.

well as destigmatising and legalising all consensual ones. But during this period, the concept, and especially the way it has been deployed in law, has also come under considerable and growing criticism from feminist philosophers. In a nutshell, as Loick (2019, p. 1) has argued, such approaches have failed "to acknowledge the specific normative structures of intimate interactions". This has foreclosed the acknowledgement of more comprehensive understandings of sexual harm while reifying social, cultural and other relations that effectively block women from power.

The challenges are multiple. First, rape laws that centre the definition of rape on the absence of consent frequently presume that individuals have a purely instrumental relationship to their bodies. Historically, rape was for long understood as a property crime, in which a father or husband was robbed of "the potentially valuable commodity of a woman of reproductive age" (Phillips, 2013, p. 42). Vestiges of such thinking of women as men's sexual property remain in law until today, for example, where, such as in India, marital rape continues to be legal. But even where it is recognised that it is the woman herself who is harmed in rape, as is increasingly the case, elements of this legacy remain. If consent often comes centre stage in rape law, this is because law often takes inspiration from conceptualisations of sexuality as property in the person, to construct rape as a matter of merely illegitimately appropriating sex. In other words, the characterisation of the event as either "sex" or "rape" hinges almost entirely on the question of whether or not there was consent to the contracting out of a body, or the invasion of a person's body as if it was a territory or a resource: rape, in these conceptualisations, is sex minus consent. Ironically, as a result, the body largerly disappears from view in the definition of rape: rape effectively becomes a harm of the (rational) mind. The affective and physical aspects of the harm caused by rape, so integral to women's experiences, as well as their links with the raped woman's psychic state, are not acknowledged in law (du Toit, 2007; Lacey, 1998).

Second, such rape laws also are framed around individualised notions of consent, which assume a "free and equal" individual, able to make "rational" decisions irrespective of their material circumstances. But radical feminists such as MacKinnon (1991), in particular, have shown how a woman's "choices" where sexual relations are concerned are always already structured by patriarchal norms. Rape, for example, tends to be conceptualised, in law and legal interactions, on male terms: the starting point tends to be that men initiate sex, which women can only passively object to. Thus, rape trials often spend considerable time investigating evidence of the use of force by the man and/or resistance on the part of the woman to infer such objections. But where sex is always already something men do to women, MacKinnon argues, it is in practice difficult for women to distinguish between rape and intercourse, as sexuality and violence are too conflated. "Consent" for enjoyment or pleasure in sexual intercourse effectively becomes an impossibility for women. Similarly, Pateman (1989) argues that, rather than standing in opposition to consensual sexual interactions, rape is in fact "the extreme expression, or an extension of, the accepted and 'natural' relation between men and women" (Pateman, 1989, p. 82). Consent, in these circumstances "cannot be distinguished from habitual acquiescence, assent, silent dissent, submission or even enforced submission" (Pateman, 1989, p. 72).

Third, by focusing on the question of consent in determining sexual harm, the law precludes a wider discussion of the possible harms of sex that was in fact consented to. West (2010), for example, has argued that consent may well be a useful mechanism to distinguish rape from sex, but has warned that the presence of consent does not necessarily mean that sex was wanted or desired, as consent might be given for all kinds of reasons. Such unwanted sex is not necessarily considered bad. But the problem with consent as it is currently conceptualised in law is that it largely removes other possible harms relating to sexual encounters from view entirely. Oblivious to the socially constructed nature of sexual consent, legal understandings of consent, rape and sexual abuse frequently fail to reflect these nuances (Cooper, 2018).

What feminists such as MacKinnon, Patemann, and many others since then, have thus highlighted is that, rather than being free and equal individuals, women, as well as sexual minorities, always come into being in a social context that is in important ways constitutive of them and frequently constructs them as effectively incapable to claim full (sexual) subjecthood. If consent is to function as a means to effectuate rights to self determination, autonomy and freedom of women, its conceptualisation and operationalisation need to take into account these social relaties. Moreover, feminists such as Hill Collins (2005) have stressed that gender is not the only factor structuring the possibility of meaningful consent: race, class, disability and sexuality, for example, all play a forceful role as well.

3.2 Strengthening Consent: A Feminist Perspective

What the previous section has made clear is that, rather than an expression of the will of autonomous and equal individuals, consent is fundamentally embedded in power relations that, legally and/or socially, construct some as free and equal, and others as less so. The consent of the latter is then irrelevant or, as in the case of marital rape, always already assumed. How, in these circumstances, can consent be strengthened?

With regard to sexual consent, du Toit (2007) has argued in a general sense that "the legal domain should concern itself with protection of the material, symbolic and other conditions necessary for the individuation of all humans in their own sexuate being, i.e., for the formation and maintenance of the kind of subject presupposed by that domain, namely a free and responsible sexual agent" (p. 59). A number of central ways that have emerged within feminism over the years to take this effort forward are as follows:

- **Consent must be embedded in a notion of relational, rather than individual, autonomy**

Many feminists have highlighted the need for a shift from an individual notion of autonomy to a relational one, if we are to understand how notions of consent can be strengthened (see e.g. Nedelsky, 1989). As Lacey (1998) has noted, "while the idea of autonomy as independence seems directly relevant to the wrong of rape, it dominates at the expense of the development of a positive conception of what kinds of sexual relationships matter to personhood" (p. 117). Where consent is embedded in notions of individual autonomy, the free and equal individual is presupposed. Where consent is understood as an aspect of relational autonomy, the ways in which consent is constituted as a meaningful possibility, or not, and thus contributes to or distracts from the attainment of full personhood, come to the fore.

Lacey (1998) herself has made efforts to move towards such an alternative conception. Building on the work of Cornell (1995), she introduces the notion of sexual integrity to highlight that to be meaningful, consent needs to be conceptualised in far broader terms than is currently the case - terms which include, among other things, an assumption of responsibility between individuals and mutuality of relationships. Others, such as Pineau (1989) and Anderson (2005), have argued for a communicative approach to consent and sexuality, which requires consultation, negotiation and reciprocity. By taking a relational view, such authors are thus exploring and finding ways to strengthen women's ability to provide meaningful consent.

A number of principles on which these alternative approaches are based deserve further attention.

- **Consent must be proactively given**

As part of the communicative approach, Pineau (1989) argues that it is imperative to communicate consent in the affirmative to each other. This may be verbal mostly, however not always. This concept was theorised to shift the burden of proof away from women, who are frequently asked to prove that they have resisted in an attempt to prevent sexual violence or rape. Communicative sexuality demands that the one requesting sexual activity, whatever their gender, has obtained the consent of the sexual partner.

Various US colleges moved towards instituting such a policy, known as a "yes means yes policy". Humphreys and Herold (2003) found that college students resented the policy and considered it regressive in times of evolution of sexual activity. The students argued that it was not possible to take consent every time, for every sexual act within a sexual encounter. This requirement, they argued, would disrupt the sexual experience. That, however, is not the goal of communicative sexuality. Rather, the concept seeks to ensure that no more the affected partner - mostly a person who is vulnerable, for example a woman, trans person, or queer person - will be required to prove that they expressed their dissent. Instead, the partner initiating the act will be required to prove beyond a doubt that they have sought consent and to demonstrate that consent was expressed.

- **Consent is specific, continuous and ongoing**

As it fails to see that sexual experiences are intersubjective, the contractual approach to consent requires sexual partners to make decisions prior to the act; the assumption is then that consent for one particular act implies consent for a number of acts. There is no option to withdraw consent, including in the middle of an act. According to this approach once a certain level of intimacy has been established, there is no going back (Cahill, 2001).

Troost (2008) argues that this assumption often comes into play because we operate on the basis of a map of consent. Such maps are structured around two sets of assumptions. First, consent for certain acts is assumed simply on the basis of the level of intimacy between the individuals concerned. And second, where one form of touch has been consented to, this is believed to imply consent to all forms that are considered to be "at its level or below" (p. 175).

One of the challenges with such maps of consent is that they "do not allow touch to be evaluated on its own or judged for how it feels at the time" (Troost, 2008, p. 175). For this reason, functioning on the basis of such maps undermines a person's sovereignty, their control over their body and self-determination. In fact, such maps may lead to victim blaming and shaming, as the partner who became uncomfortable during an act and wished to withdraw might blame themselves or be shamed that they first consented - why then did they complain later (Alcoff, 2009)? Where these maps are based on anatomy, they in addition lead to the objectification of the person touched, undermining their ability to seek pleasure on their own terms (Troost, 2008).

Consent, however, cannot be assumed to be a blanket "yes" for the whole act; it is to be sought for different acts and at different stages. Consent is required to be built. After all, as sexual experiences are embodied and often spontaneous, partners decide in the very moment if the touch is comforting, desirable or not (Cahill, 2001). Consent cannot be pre-decided or controlled by someone else. For example, affirmative consent to kissing or foreplay does not amount to consent to penetrative intercourse ("Acquaintance rape and degrees of consent: 'no' means 'no', but what does 'yes' mean?", 2004). Further, consent received on past occasions cannot be presumed for current or future instances.

This concept of ongoing consent does not mean to devalue past or existing relationships, but intends to ensure that consent must be present, continuous and ongoing (Gruber, 2016).

- **Consent is a process**

What the above section already highlights is that consent is also a process. But this goes beyond the question of whether to have sex or engage in a particular act. A communicative approach to consent also opens up a conversation about what shape that should take, and why a person might like something or not, as well as the space to say "maybe" as part of that exploration. As Bussel (2008, p. 43) argues, "without our speaking up and demanding that our lovers do, too, we don't ever truly know what they are thinking, which impedes us from having the sex we could be having".

Thus, thinkers such as Bussel mobilise consent as a tool to break the silence in between yes and no as well: consent moves from being a yes/no question to involving a process aimed at truly knowing as well as respecting another person in all their complexity. Consent becomes the bedrock of a true partnership.

- **Consent allows for negotiation by all parties involved**

Following on from the above, it is clear that consent also requires the ability to negotiate.

As discussed, dominant perceptions of consent as per the hetero-patriarchal regime hold that one person (mostly a man) initiates a sexual act and seeks consent from the other (often a woman). The roles of both partners have been fixed by the virtue of their genders and have been normalised following the norms of the society (Beres et al., 2004). As a result, there is no real negotiation between the partners. Maps of consent further play into this.

The concept of consent, when understood in this way, places boundaries on how we understand heterosexual interactions, as well as limiting our ability to seriously address sexual violence in homosexual relationships. In contrast, Braun, Gavey and McPhillips (2003) argue, and the previous section also made clear, that consent requires mutual negotiations, which enable equality and respect. Reciprocity allows partners to gratify each other's sexual experience by accounting for each other's desires. Thus, to enable negotiations in consent seeking, it is imperative to imbibe the principle of reciprocity.

For each partner to be able to participate in such negotiations, it is, however, essential that they are able to say no. You need to be able to walk away from a negotiation if you are to be effective. At the same time, and as also alluded to by the previous section, this is not enough. For consent to be meaningful, it also requires an ability to provide input on the terms of agreement. Merely being able to say yes or no to a proposal a person is presented with does not suffice.

- **Conditions must be created so that consent can be given freely**

Consent is very intimate, it cannot be given on behalf of someone else. Only the individual from whom it is requested can express their willingness. However, to be meaningful, as Hickman and Muehlenhard (1999) argue, consent must also be "free" from any physical or psychological encumbrance at the time when it is expressed.

In practice, as discussed above, not everyone can give consent freely in all circumstances. The assumption that all humans are free and autonomous is flawed and does not consider the asymmetrical power relations that structure society. The capacity as well as opportunity to meaningfully consent is constrained by an individual's location in historical, social systems of oppression that are stratified by a range of structural factors, including gender, age, caste, race, class, sexuality and disability. Because of such asymmetrical power relations, it may be easier to violate the ability to express or deny consent of some individuals than that of others. Moreover, systems of oppression, whether based on physical, social, political or economic inequalities, may use this power imbalance to compel an individual to give consent (Peña & Varon, 2019). As a result, consent loses its essence and becomes a means to inflict oppression and violence.

For example, in the context of India, Dalit women occupy particularly vulnerable economic, social and cultural locations, undermining in practice their capacity to meaningfully express or deny consent (Munuswamy, 2020). This further works to aggravate the sense of impunity with which perpetrators inflict violence on them (Sen, 2020). Asymmetrical power relations also inhere to specific situations, such as those of a classroom setting or a workplace, in which the individual that is subordinate may be compelled to consent by virtue of their relative lack of knowledge and power. That consent, too, cannot be termed "free" from encumbrances. In still other situations, such as when a teenager engages in sexual acts because of peer pressure rather than because they wish to, the social forces at play may be less apparent or tangible, yet still play a significant role in decision making.

Thus, to enable meaningful consent, it is essential that power relations are not merely understood, but addressed. Only then can the person from whom consent is sought be empowered to give as well as refuse consent. This brings us back to the point that we started with: consent needs to be conceptualised as embedded in not individual, but relational autonomy if it is to bring us closer to the ideal of the "free and equal" individual, rather than presume that we already fit that ideal before giving consent.

In summary, from a feminist perspective, the following qualifiers to ascertain meaningful consent can, thus, be deduced:

- Consent must be embedded in a notion of relational, rather than individual, autonomy.
- Consent must be given proactively, communicated in the affirmative.
- Consent must be specific, continuous and ongoing, to be sought for different acts and at different stages. Consent is required to be built.
- Consent is a process, and thus opens up a conversation, rather than entailing merely a yes/no decision.
- Consent allows for negotiation by all parties involved; this requires the ability for each party to say no as well as to provide input on the terms of agreement.
- Conditions must be created so that consent can be given freely. This implies that the person should be free from any fear of oppression or violence of any kind.

4. Rethinking Consent in Data Protection

4.1 Lessons from Feminist Perspectives on Consent for Data Protection

What lessons do these feminist critiques of consent teach us where the debate on data protection is concerned? Once the need to put bodies back into the data debate is recognised and data is redefined as property in the person, the parallels are striking.

In the most general sense, they highlight how consent, aided by the fiction of data as a resource, comes to function as a legitimisation of a new set of power relations both ideologically and in practice, while obscuring a broader set of harms. The fact that those consenting never had the power to influence how this consent is defined, where it begins and ends, or what it looks like is left out of legal consideration, as is the question of whether those consenting ever had the option not to consent. Thus, every time we tick that consent box, we are reminded, following Brown (1995, p. 162-163), of "the presence of a power... that one does not oneself create, but to which one submits".

Moreover, in that process, the question cannot even be asked how the practices that a person is supposedly consenting to undermine the formation of that very person as a free and responsible agent - even if (or perhaps precisely because) that same practice of consent effectively already *assumes* that the person consenting is such a free and equal agent. So many of these debates continue to be phrased around the fiction of data as a resource, which is then treated as a contractible property in the person; as a consequence, for the moment, we often do not even have a common vocabulary to talk about harms, their causes, and the change needed. Dominant conceptualisations of data and consent simply prevent us from developing the language or imaginary to raise critical questions.

By individualising the burden of taking decisions through consent, we are, thus, depoliticising, even invisibising, the impact of existing data infrastructures, and the power relations that structure them, on our bodies and lives.

What would it mean, in contrast, to adopt a feminist approach to consent that recognises the entanglement between our bodies and data in data protection regimes? At first sight, it may seem like some of the qualifiers are already common to both regimes, in particular those that specify that consent should be free, informed, specific, easy to withdraw and affirmative. However, current data protection regimes do not put these principles into practice. In section two of this paper, we observed that data protection regimes currently approach the notice and consent model as a means to enable "privacy self management" (Solove, 2013), and noted that the conditions identified by the current data governance regimes for seeking consent are flawed. This is because these frameworks are oblivious to the structural obstacles faced by those whose consent is sought. A re-examination of consent that takes integrity of the self as its starting point makes clear that to strengthen the quality of consent, the consent qualifiers need to undergo a change.

In particular, current data protection frameworks perceive privacy strictly as an individual right, independent of context and socio-political environment. In contrast, as we have seen, when examining autonomy in terms of consent, feminists have highlighted that the autonomy of individuals is relational in nature (Nedelsky, 1989). Individuals may be autonomous, however their ability to exercise that autonomy is contingent upon their social context. Merely tinkering with the operationalisation of consent will then not be enough: what is required is a reconceptualisation of consent.

Or to put it in other words, the task currently before us is, first of all, to locate historically the processes of subjectification, including the structure of consensual acts, that are built into datafication, and, then, to change these in ways that ensure the opportunity for all to grow in practice into the free and equal human beings that we are already assumed to be in theory (Drakopoulou, 2007). In particular, such interventions will need to focus on challenging the new relations of subordination that have *de facto* come into existence and have transformed all our lives (Zuboff, 2019) as a consequence of the treatment of data as a new form of property in the person that can safely be brought under contract. Moreover, although these changes affect all of us, this is especially important for those of us who are already vulnerable or marginalised in some way. The extensive knowledge and information that a growing number of data controllers have about their users confers them with considerable power over these individuals, further disadvantaging those already marginalised (Malgieri & Niklas, 2020). If all users are to express their will "freely", it is imperative to be cognisant of these vulnerabilities.

Such views are put forward sporadically by critics of current data protection debates as well. Cohen (2019), for example, has argued that placing individualised control at the centre of consent has proven to be a fundamental failure in conceptualising consent in data protection regimes. She states that "selfhood is a product of both social shaping and embodied experience" (p. 9). An individual is born in a social context, and this cannot be overlooked while evaluating an individual's selfhood. In order to acknowledge the inequitable distribution of power and to uphold the existing principles of consent in data protection frameworks, Cohen (2019) therefore argues that privacy should be approached in a condition-centric manner rather than a subject-centred manner. In the next section we will examine more concretely what a feminist perspective on consent can teach us about how to strenghten current regimes.

4.2 Moving towards Concrete Proposals for Change

It is impossible to present in detail all changes that would be required in order to ensure that consent in data governance contains at least a modicum of meaningfulness - nor, in fact, do we want to claim that we possess full knowledge of all changes needed at this time. It is difficult to have such a comprehensive sense of what the road ahead should look like when in the middle of a paradigm shift and when we, as noted, frequently even lack the vocabulary to name the changing realities that we see taking shape around us. But on the basis of the preceding discussions, it is possible to already propose a number of changes that should be made immediately. After all, whether state-supported or primarily private sector driven, it is clear that the logic of surveillance capitalism is deeply harmful to the autonomy and dignity of the individual. Not only do we have extremely limited powers to negotiate at the time of data collection, once consented to that data being collected, we also have no ability to influence how it will be used. In other words, "the consequence of contracting out part of property in the person is that a diminution of autonomy or self-government occurs" (Pateman, 2002, p. 33). Regulation should therefore be put in place to end all such harmful practices, including by putting restrictions, if required, on the business models that companies can adopt. At least three different types of changes need to be made.

- **Changes required at the time when data is collected**

It is evident from earlier sections that in order to translate the reconceptualisation of personal data as an extension of bodies into the existing privacy regime, data collection practices need to be revisited and re-modelled. Although at present data protection regimes often contain the principles of data minimisation and purpose limitation, such purposes have been decided by the data controller or data

fiduciary, either state actors or non-state actors, rather than the individual seeking to buy a product or use a service. These purposes are not always aligned with those the user has in mind. In fact, as Zuboff (2019) has argued, in the age of surveillance capitalism, they generally aren't.

As explained earlier, while in the early stages of the Internet's development, user data was collected to be able to improve the products or services they used, today the focus of most companies is on getting access to what Zuboff (2019) calls our "behavioural surplus": all the data generated while we engage with technology that has no value where improving the service is concerned, but that can be used to make predictions about our future behaviour and be sold to advertisers and others. Thus, while users are made to believe that they are signing up to use a particular service or product, instead they are often signing away control over their data bodies to the data controller in one click. For example, the popular augmented reality game, Pokémon Go, is generally understood by players as a game to be played not on a screen but in the real world. However, developer Niantic and other big companies, including Mc Donald's and Starbucks, envisioned the game as a tool to engineer and change individuals' behaviour, drawing on the app's behavioural surplus. The app collects copious amounts of data about its users, such as their gender, continuous location, activities they engage in while using the app, etc. Using this data, Niantic put into place a system of rewards and penalties which incentivises players to visit certain places, buy certain goods and engage in certain activities. Thus, users are lured to spend time, money and energy while catching pokemons (Zuboff, 2019).

This practice of accumulating an individual's behaviour surplus is not limited to the private sector: some states have also been deploying these deceptive surveillance capitalism techniques under the garb of providing services and ensuring security. They may also have been selling personal and sensitive personal data of individuals to private entities in order to make profits. For example, in India, the Economic Survey 2018-2019 (Department of Economic Affairs, 2018) included statements conveying how data can be used by the state to generate revenue. Moreover, this was not merely hypothetical: the Ministry of Road Transport and Highway has acknowledged in a series of parliamentary questions that the Ministry has already sold the *Vahan* and *Sarathi* data, or the vehicle registration and driving license data, of Indian individuals to private entities for INR 3 crore, or more than USD 400 000 (Singh, 2019).

In these circumstances, to what extent consent can be considered to have been specific is therefore questionable. Many users still are not familiar with the operations of surveillance capitalism even in broad terms, and the user agreements that they sign do little to enlighten them. A first step to making consent meaningful would therefore be to put an end to these deceptive and opaque practices that disable people from learning what they actually signed up for.

Merely shedding light on the practices of the data controllers is, however, not enough. For consent to be meaningful, it should be possible for a user to say no to any practice that doesn't relate narrowly to the service being provided - this is what it would mean to be able to negotiate the terms of the agreement. As highlighted above, if consent is to be thought of not merely as a yes/no binary but as an ongoing activity and conversation, it is essential that mechanisms are provided that enable the individual to engage in negotiations before, during and after giving consent.

At present, of course, the ability to negotiate barely exists. Though some jurisdictions allow users to make small adjustments (for example, to cookie settings), consent forms generally are take-it-or-leave it arrangements that force users to accept extensive surveillance both by the data controller and third parties. Moreover, after users have consented, data controllers can unilaterally change privacy policies in ways that further disadvantage users, with the only option for users to agree or stop using the service. To facilitate meaningful consent, an end should thus be put to these practices as well.

Further, there are jurisdictions and privacy policies that enable data controllers to process the personal data of individuals for "certain reasonable purposes" not explicitly mentioned in their privacy policies. It is either the state or the private corporations that decide what these "reasonable purposes" entail, thus again demeaning the ability of individuals to provide meaningful consent, or to negotiate. India's draft Data Protection Bill, 2019, for example, contains such a provision.

While mechanisms such as the right to access your data or to correct it have been rolled out in some jurisdictions, in many parts of the world they remain inexistent, leaving users often without even the possibility to get insight into what data a data controller has about them.

Finally, in some situations, the notice and consent requirement is commonly done away with altogether. For example, as the state is responsible for providing essential services such as subsidies, licenses, and security to its citizens, the relationship between the state and its citizens is unique. Thus, consent is often not sought for collecting and processing of data by the state for security of the state or in cases of emergency or for the provision of essential services.

It may be true that the state may not be able to seek consent of the individuals to collect and analyse their personal data for the purpose of the security of the state. However, in other situations, such as for the provision of essential services and in emergencies, at the very least notice should be provided wherever feasible - not in the least because this can be a tool to improve transparency, and ask for accountability, concerning governments' data collection efforts. In addition, individuals should be able to negotiate with the state: in particular, they should be asked for, and be able to deny, consent to data sharing for any non-essential purpose, including advertising, marketing, and even research, at the time of data collection. Moreover, such consent should be sought for each non-essential purpose separately, and these purposes should be clearly and narrowly defined. Finally, denying consent for data collection and processing for non-essential purposes may not amount to exclusion from goods and services that are essential to life and to which citizens have a right under the country's Constitution, nor may such a denial have any other negative repercussions for citizens.

In general, data governance policies need to demarcate more narrowly situations in which the requirement to provide notices and seek consent can be done away with in the first place.

- **Changes required to what are permissible uses of collected data**

As the above makes clear, where mechanisms to negotiate exist, they seem to focus squarely on the data that the user shares with the data controller. But negotiation in terms of what the data controller does with this data is impossible, even if such processes undermine the individual's autonomy and sovereignty. A second set of changes are thus required to ensure that we will never even be asked to consent to certain currently widely adopted practices in the first place; these practices should simply no longer be legal.

Of particular concern are the many hidden and not-so-hidden strategies that data controllers use to manipulate users, generally in the name of micro-targeting[2] (Sunstein, 2016). Sometimes, this takes seemingly innocuous forms. For example, trackers on many websites, including YouTube, provide for "yes" or "not now" as the only options to avail services. In other words, it is impossible for a user to

[2] Cass Sunstein (2016) defines manipulative actions as intentional acts to influence individuals that fail to take into consideration or appeal to the individual's capacity for reflection and deliberation.

completely deny consent or choose “no”. While this may seem quite innocent, such techniques are meant to habituate us to the pervasiveness of tracking, to make it seem natural, something we only temporarily will not allow a data controller to engage in.

In other cases, the potential impact and harms of such techniques can be far more dangerous, however. This is true especially where they aim to identify vulnerabilities and cognitive biases of individuals to exploit them. When does “nudging” actually become “manipulation”? And how do we know it has crossed that line (Susser et al., 2019)? At present, it is impossible for us to find out when we are being targeted by such techniques.

In order to restore our autonomy and sovereignty as individuals with regard to our datafied bodies, existing business and governance models that seek profit or a boost in surveillance capacity, including for welfare purposes, from analysing behavioural surplus should therefore be disallowed. The only exception can be where, following extensive public debate, there is societal agreement, subsequently translated into law, that this serves the public good.

For similar reasons, an end should also be put to practices which deny users the possibility to object to third party data sharing, yet refuse to take up any responsibility for harms that may accrue to the user following such data sharing or, equally damaging, simply presume that consent implies consent to the terms and conditions of all these third parties as well. Unless consent qualifiers that have been fleshed out from a feminist perspective can and are applied separately and explicity to third party data sharing as well, such practices should be prohibited too. Moreover, such a prohibition should be applied to the selling of citizens' raw and aggregated data, including behavioural surplus, by governments as much as by the private sector, and whether to private or public entities. Data sharing by government, including among government departments, too, should be prohibited, unless such sharing is essential to, for example, the provision of the service requested and to which this data relates.

For example, the privacy policy of Aarogya Setu, a contact tracing application to address the COVID19 pandemic first launched by the Government of India in April 2020,[3] currently states that users' personal information may be shared with third parties or other persons as the state deems fit, for medical or administrative interventions.[4] The terms “medical” and “administrative” are not defined in the notice of the application. As these are potentially very wide in scope, they can be easily misused. Thus, the policy in its current form fails to provide users with the ability to meaningfully consent to all aspects of the app, or to allow its users to negotiate with terms like “third party data sharing”. Going forward, such broad data sharing clauses should no longer be allowed.

- **Changes required to especially protect people who are particularly vulnerable**

While the above are changes that are required to protect all of us, for some people, in some situations, additional protections may be required. After all, if vulnerabilities are only approached in a generalistic manner, where vulnerability is believed to be a universal characteristic applicable to all of us, this will often be at the expense of recognising the specific conditions of those who are already marginalised and discriminated against (Malgieri & Niklas, 2020). This need to provide additional protections for those particularly vulnerable is already widely recognised in data protection regimes where, for example, children are concerned. But additional protections may need to be considered for other groups, sometimes in particular situations, as well.

[3] Aarogya Setu app, https://www.mygov.in/aarogya-setu-app/

[4] Privacy Policy, Aarogya Setu app, https://web.swaraksha.gov.in/ncv19/privacy/

Luna (2019) proposes that we pay attention to two factors when assessing vulnerability and determining whether additional protections might be required: the likelihood of risks and the harmfulness of effects. Where consent is concerned, this may lead to additional protections both where the collection of data and the use of data are concerned. For example, where data is collected as part of the employer-employee relationship, people might be in a situation of decisional vulnerability as there is a clear power imbalance between themselves and those collecting the data (Jain et al., 2020). Thus, because of employees' decisional vulnerability, consent becomes a weak ground for the collection and processing of data (Malgieri & Niklas, 2020). Yet this decisional vulnerability can be mitigated through a range of measures. For example, employers should provide notice to employees on the kind of data they collect, to improve transparency and the possibility to demand accountability. In addition, mechanisms could be put into place to strengthen the sector-wise collective bargaining power of employees with regard to work-related data collection and processing. These could be complemented by co-regulatory processes which would require industry-specific employers to draft consent regimes in cooperation with employees and/or trade unions and which would be subject to approval by data protection authorities. Finally, the principles of permissible work-place surveillance - both in terms of the data collected and the forms of processing that are allowed - should be outlined in law. Practices that undermine the dignity, autonomy and bodily integrity of employees, such as algorithms that try to deduce employees' mental health status, should be prohibited.

These are only some of the many changes that would need to be made to data governance regimes in order to ensure that the sovereignty of our datafied bodies is not continuously violated. The challenge with consent in the digital age is not that consent has become impossible to operationalise. While it may well be true that it can never do all the work that we expect from it, at the moment the bigger issue is that the structural conditions that allow for consent in data governance to be meaningful have not been put in place. A feminist perspective on consent in the age of embodied data makes clear how a beginning to such changes can be made.

Conclusion

While consent continues to be a crucial element of data protection regimes around the world, it has also been diagnosed with numerable weaknesses as a tool to promote and protect individuals' autonomy, and has therefore come under considerable and growing criticism. In this paper, we set out to learn from feminist theory around consent in general, and feminist applied thinking around sexual consent in particular, how consent regimes in data protection can be strengthened. We argued that such a journey would be promising because of the close entanglements between our bodies and our data. We particularly foregrounded feminist criticisms of “property in the person” to understand in more detail the deep harms that current data practices do to our personhood, as well as the ways in which consent is currently deployed to enable and even legitimise such practices, rather than challenge or reject them. Through close engagement with feminist thinking around consent, we then developed a list of feminist principles that will need to be followed if consent is to ever be meaningful in the governance of data that is closely entangled with our bodies. Finally, we outlined three areas of change that the application of these principles immediately points to: changes related to the collection of data; changes related to the uses of data; and changes required to protect people who are especially vulnerable in particular.

As in sexual relations, putting each of the feminist principles of consent fully into practice in data governance may not necessarily be easy or straightforward. Doing so requires us to examine and address power imbalances not only in the laws that govern our consent, but in the design, code and

political economy of the data infrastructures that shape our possibilities for consent as well - keeping in mind throughout the close entanglement between our bodies and data. Some challenges may be simpler to tackle than others. Some may require so many shifts in our current thought and practices that it will likely take years to fully see these changes' positive impact. Some, we may never be able to fully overcome. Yet what the feminists principles of consent outlined in this paper provide us with is a blueprint of the direction in which we need to move if we are to ensure that, rather than enabling new and pervasive forms of subordination, the data relations of the future will empower each and everyone of us. Instead of subordination, the feminist principles of consent help us to imagine the shape of data relations that allow people to actually move closer to the ideal of the “free and equal” subject. By developing a feminist perspective on consent in data governance that takes into account the close entanglements between data and bodies, it is this project of democratisation that this paper ultimately hopes to have contributed to.

List of References

Acquaintance rape and degrees of consent: "no" means "no," but what does "yes" mean? (2004). *Harvard Law Review*, 117(7), 2341-2364. DOI: 10.2307/4093340.

Ackerly, Brooke A. (2008). Human rights and the epistemology of social contract theory. In Daniel I. O'Neill, Mary Lyndon Shanley, & Iris Marion Young (Eds.), *Illusion of consent: Engaging with Carole Pateman* (pp. 75-95). Pennsylvania State University Press.

Acquisti, Alessandro, John, Leslie. K & Loewenstein, George (2013). What is privacy worth? *Journal of Legal Studies*, 42(2), 249-274. DOI: 10.1086/671754

Alcoff, Martin Linda (2009). Discourses of sexual violence in a global framework. *Philosophical Topics,* 37(2), 123-139. http://www.jstor.org/stable/43154560

Anderson, Michelle J. (2005). Negotiating sex. *Southern California Law Review,* 78(6). https://core.ac.uk/download/pdf/229258185.pdf

Article 29 Data Protection Working Party (2012). *Opinion 02/2012 on facial recognition in online and mobile services* (00727/12/EN WP 192). European Commission. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp192_en.pdf

Bailey, Rishab, Parsheera, Smriti, Rahman, Faiza, & Sane, Renuka (2018). *Disclosures in privacy policies: Does "notice and consent" work?* (Working Paper Series, 246). National Institute of Public Finance and Policy. https://www.nipfp.org.in/media/medialibrary/2018/12/WP_246.pdf

Barocas, Solon & Nissenbaum, Helen (2014) Big data's end run around anonymity and consent. In Julia Lane, Victoria Stodden, Stefan Bender & Helen Nissenbaum (Eds.), *Privacy, big data, and the public good frameworks for engagement* (pp 44-75). Cambridge University Press. DOI: 10.1017/CBO9781107590205.004

Barocas, Solon & Nissenbaum, Helen (2009). On notice: The trouble with notice and consent. *Proceedings of the Engaging Data Forum: The First International Forum on the Application and Management of Personal Electronic Information.* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2567409

Beres, Melanie Ann, Herold, Edward & Maitland, Scott B. (2004). Sexual consent behaviors in same-sex relationships. *Archives of Sexual Behavior,* 33(5), 475–86. DOI: 10.1023/B:ASEB.0000037428.41757.10

Braun, Virginia, Gavey, Nicola & McPhillips, Kathryn (2003). The `fair deal'? Unpacking accounts of reciprocity in heterosex. *Sexualities,* 6(2), 237-261. DOI: 10.1177/1363460703006002005

Brown, Wendy (1995). *States of injury: Power and freedom in late modernity.* Princeton University Press.

Bussel, Rachel Kramer. (2008). Beyond yes or no: Consent as sexual process. In Jaclyn Friedman & Jessica Valenti (Eds.), *Yes means yes! Visions of female sexual power & a world without rape* (pp. 43-52). Seal Press.

Cahill, Ann J. (2001). *Rethinking rape.* Cornell University Press.

Cate, Fred H. & Mayer-Schönberger, Viktor (2013). Notice and consent in a world of big data. *International Data Privacy Law,* 3(2), 67–73. DOI: 10.1093/idpl/ipt005

Cohen, Julie E. (2019). Turning privacy inside out. *Theoretical Inquiries in Law,* 20(1). https://ssrn.com/abstract=3162178

Cooper, Chiara (2018). Speaking the unspeakable? Nicola Lacey's unspeakable subjects and consent in the age of #metoo. *Feminists@Law*, 8(2). DOI: 10.22024/UniKent/03/fal.669

Cornell, Drucilla (1995). *The imaginary domain: Abortion, pornography and sexual harassment.* Routledge.

Couldry, Nick & Mejias, Ulises. A. (2019). *The costs of connection: How data is colonising human life and appropriating it for capitalism.* Stanford University Press.

Council of Europe (1981). *Convention for the protection of individuals with regard to automatic processing of personal data* (ETS No. 108). Treaty Office, Council of Europe. https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37

Custers, Bart, Dechesne, Francien, Pieters, Wolter, Schermer, Bart Willem, & van der Hof, Simone (2019). Consent and privacy. *The Routledge Handbook of the Ethics of Consent* (pp. 247-258). Routledge.

Custers, Bart, van der Hof, Simone, & Schermer, Bart Willem. (2014). Privacy expectations of social media users: The role of informed consent in privacy policies. *Policy and Internet,* 6(3), 268-295. DOI: 10.1002/1944-2866.POI366

Davis, Nathan J. (2007). Presumed assent: The judicial acceptance of clickwrap. *Berkeley Technology Law Journal,* 22(1), 577–598. http://www.jstor.org/stable/24118246

Davis, Peter (2020). Facial detection and smart billboards: Analysing the "identified" criterion of personal data in the GDPR. *University of Oslo Faculty of Law,* Research Paper No. 2020-01. DOI: 10.2139/ssrn.3523109

Department of Economic Affairs (2018). *Economic Survey 2018-2019* (Volume 1). Ministry of Finance, Government of India. https://www.indiabudget.gov.in/budget2019-20/economicsurvey/doc/echapter.pdf

Drakopoulou, Maria (2007). Feminism and consent: A genealogical inquiry. In Rosemary Hunter & Sharon Cowan (Eds.), *Choice and consent: Feminist engagements with law and subjectivity* (pp. 9-38). Routledge-Cavendish.

du Toit, Louise (2007). The conditions of consent. In Rosemary Hunter & Sharon Cowan (Eds), *Choice and consent: Feminist engagements with law and subjectivity* (pp. 58-73). Routledge-Cavendish.

Directorate-General for Justice and Consumers (2015). *Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content.* (Brussels, COM/2015/0634 final - 2015/0287 COD). European Commission. ec.europa.eu › rep › 1 › 2015 › 1-2015-634-EN-F

Fairfield, Joshua A.T. & Engel, Christoph (2015). Privacy as a public good. *Duke Law Journal,* 65(3), 385-457. https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=3824&context=dlj

Goffman, Erving (1959). *The presentation of self in everyday life.* Doubleday.

Gruber, Aya (2016). Consent confusion. *Cardozo Law Review,* 38 (2), 415-457. https://scholar.law.colorado.edu/articles/11

Hayles, Katherine N. (1999). *How we became posthuman: Virtual bodies in cybernetics, literature, and informatics.* University of Chicago Press.

Heaven, Douglas (2020, February 26). Why faces don't always tell the truth about feelings. *Nature.* https://www.nature.com/articles/d41586-020-00507-5

Hermstrüwer, Yoan (2017). Contracting around privacy: The (behavioral) law and economics of consent and big data. *Journal of Intellectual Property, Information Technology and E-Commerce Law,* 8(1), 8-26. https://www.jipitec.eu/issues/jipitec-8-1-2017/4529/JIPITEC_8_1_2017_Hermstruewer.pdf

Hickman, Susan E. & Muehlenhard, Charlene L. (1999). "By the semi-mystical appearance of a condom": How young women and men communicate sexual consent in heterosexual situations. *Journal of Sex Research,* 36(3), 258-272. www.jstor.org/stable/3813437

Hill Collins, Patricia (2005). *Black sexual politics: African Americans, gender, and the new racism.* Routledge.

Humphreys, Terry, & Herold, Ed (2003). Should universities and colleges mandate sexual behavior? *Journal of Psychology & Human Sexuality,* 15(1), 35-51. DOI: 10.1300/J056v15n01_04

Jain, Tripti, Kovacs, Anja & Ranjit, Tanisha (2020). *Submission to the Joint Parliamentary Committee on the Personal Data Protection Bill 2019.* Internet Democracy Project.

Jernigan, Carter, & Mistree, Behram F. (2009). Gaydar: Facebook friendships expose sexual orientation. *First Monday,* 14(10). DOI: 10.5210/fm.v14i10.2611

Joint Committee on Human Rights (2019). *The right to privacy (Article 8) and the digital revolution* (Third report of session 2019, HC 122, HL Paper 14). House of Commons and House of Lords. https://publications.parliament.uk/pa/jt201919/jtselect/jtrights/122/122.pdf

Jolls, Christine & Sunstein, Cass R. (2005). *Debiasing through law* (Working Paper no. 11738). National Bureau of Economics Research. http://www.nber.org/papers/w11738

Kovacs, Anja & Ranganathan, Nayantara (2019). *Data sovereignty, of whom? Limits and suitability of sovereignty frameworks for data in India* (Working Paper No. 3). Data Governance Network. https://datagovernance.org/report/data-sovereignty

Lacey, Nicola (1998). *Unspeakable subjects: Feminist essays in legal and social theory.* Hart Publishing.

Libert, Timothy. (2018l). An automated approach to auditing disclosure of third-party data collection in website privacy policies. In *Proceedings of the 2018 World Wide Web Conference* (pp. 207–216). International World Wide Web Conferences Steering Committee. DOI: 10.1145/3178876.3186087

Locke, John (1988). *Two treatises of Government* (Peter Laslett, Ed.). Cambridge University Press. (Original work published 1689)

Loick, Daniel (2019). "... As if it were a thing." A feminist critique of consent. *Constellations,* 1-11. DOI: 10.1111/1467-8675.12421

Luna, Florencia (2019). Identifying and evaluating layers of vulnerability: A way forward. *Developing World Bioethics,* 19(2), 86-95. DOI: 10.1111/dewb.12206

MacCarthy, Mark (2011). New Directions in privacy: Disclosure, unfairness and externalities. *6 I/S: A Journal of Law and Policy for the Information Society,* 6(3), 425-512. Available at SSRN: https://ssrn.com/abstract=3093301

MacKinnon, Catherine A. (1991). *Towards a feminist theory of the state.* Harvard University Press.

Malgieri, Gianclaudio & Jędrzej Niklas (2020). Vulnerable data subjects. *Computer Law & Security Review,* 37. DOI: 10.1016/j.clsr.2020.105415

Mandel, Michael (2017). *The economic impact of data: Why data is not like oil.* Progressive Policy Institute. https://www.progressivepolicy.org/wp-content/uploads/2017/07/PowerofData-Report_2017.pdf

Matthan, Rahul. (2017, July 19). *Beyond consent: A new paradigm for data protection* (Discussion Document 2017-03). The Takshashila Institution. https://takshashila.org.in/wp-content/uploads/2017/07/TDD-Beyond-Consent-Data-Protection-RM-2017-03.pdf

MIT Technology Review Insights. (2016). *The rise of data capital.* MIT Technology Review. https://www.technologyreview.com/s/601081/the-rise-of-data-capital/

Munuswamy, Kiruba. (2020, October 6). When I rage over Hathras, why call it 'personal' & 'Dalit anger'? *The Quint.* https://www.thequint.com/voices/opinion/hathras-rape-dalit-woman-caste-atrocities-thakur-supremacy-violence-uttar-pradesh-police-state

Nedelsky, Jennifer (1989). Reconceiving autonomy: Sources, thoughts and possibilities. *Yale Journal of Law and Feminism,* 1(1), 7-36. https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1004&context=yjlf

National Telecommunications and Information Administration (2010). *Notice on information privacy and innovation in the internet economy* (21226–2123, ISSN 0097–6326, Volume 75/78). Office of the Federal Register, National Archives and Records Administration, Washington, DC. 21229. https://www.govinfo.gov/content/pkg/FR-2010-04-23/pdf/FR-2010-04-23.pdf

OECD Council (1980). *OECD Guidelines on the protection of privacy and transborder flows of personal data* (1980 Guidelines). Organisation For Economic Co-operation and Development. https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

Okoyomon, Ehimare, Samarin, Nikita, Wijesekera, Primal, Elazari Bar On, Amit., Vallina-Rodriguez, Narseo, Reyes, Irwin, Feal, Álvaro, & Egelman, Serge (2019, May 23). *On the ridiculousness of notice and consent: Contradictions in app privacy policies.* [Workshop or Conference Paper] ConPro 2019, in conjunction with IEEE Symposium on Security and Privacy, San Francisco, CA, USA. https://eprints.networks.imdea.org/1967/

Patella-Rey, PJ. (2018). Beyond privacy: Bodily integrity as an alternative framework for understanding non-consensual pornography. *Information, Communication & Society,* 21(5), 786-791. DOI: 10.1080/1369118X.2018.1428653

Pateman, Carole (2002). Self-ownership and property in the person: Democratisation and a tale of two concepts. *Journal of Political Philosophy,* 10(1), 20-53. DOI: 10.1111/1467-9760.00141

Pateman, Carole (1989). *The disorder of women: Democracy, feminism and political theory.* Polity Press.

Pateman, Carole. (1988). *The sexual contract.* Stanford University Press.

Pearson, Jordan. (2014, September 24). Your friends' online connections can reveal your sexual orientation. *Vice.* https://www.vice.com/en/article/gvydky/your-friends-online-connections-can-reveal-your-sexual-orientation

Peña, Paz, & Varon, Joana (2019). *Consent to our data bodies: Lessons from feminist theories to enforce data protection.* Coding Rights. https://codingrights.org/docs/ConsentToOurDataBodies.pdf

Phillips, Anne (2013). *Our bodies, whose property?* Princeton University Press.

Pineau, Lois (1989). Date rape: A feminist analysis. *Law and Philosophy,* 8(2), 217-243. DOI: 10.2307/3504696

Quividi (2019). *We believe in consumer privacy.* https://quividi.com/privacy/#

Quodling, Andrew. (2018, April 13). Shadow profiles: Facebook knows about you, even if you're not on Facebook. *The Conversation.* https://theconversation.com/shadow-profiles-facebook-knows-about-you-even-if-youre-not-on-facebook-94804

Ranjit, Tanisha (2020, August 10). At stake is our bodily integrity. *The Hindu.* https://www.thehindu.com/opinion/op-ed/at-stake-is-our-bodily-integrity/article32310774.ece

Regan, Priscilla M. (1995). *Legislating privacy: Technology, social values, and public policy.* University of North Carolina Press.

Richardson, Janice (2010). Feminism, property in the person and concepts of self. *British Journal of Politics and International Relations,* 12: 56–71. DOI: 10.1111/j.1467-856X.2009.00393.x

Singer, Natasha. (2012, June 16). You for sale: Mapping, and sharing, the consumer genome. *New York Times.* https://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html

Singh, Varun (2019, July 10). Govt selling vehicle and DL data of Indians for Rs 3 crore, 87 private companies already bought. *India Today.* https://www.indiatoday.in/auto/latest-auto-news/story/govt-selling-vehicle-and-dl-data-of-indians-for-rs-3-crore-87-private-companies-already-bought-it-1565901-2019-07-10

Solove, Daniel J. (2013). Introduction: Privacy self-management and the consent dilemma. *Harvard Law Review,* 126(7), 1880-1903. https://harvardlawreview.org/wp-content/uploads/pdfs/vol126_solove.pdf

Solove, Daniel. J. (2004). *The digital person: Technology and privacy in the information age.* New York University Press.

Smith, David W. (2018, June 4). The future of advertising, or a surveillance nightmare? *Eureka.* https://eureka.eu.com/gdpr/future-of-advertising/

Sunstein, Cass R. (2016) Fifty shades of manipulation. *Journal Marketing Behavior,* 1(3-4), 213-244. DOI: 10.1561/107.00000014

Susser, Daniel, Roessler, Beat., & Nissenbaum, Helen (2019). Technology, autonomy, and manipulation. *Internet Policy Review,* 8(2). DOI: 10.14763/2019.2.1410

Troost, Hazel/Cedar (2008). Reclaiming touch: Rape culture, explicit verbal consent, and body sovereignty. In Jaclyn Friedman & Jessica Valenti (Eds.), *Yes means yes! Visions of female sexual power & a world without rape* (pp.171-177). Seal Press.

van der Ploeg, Irma (2012). The body as data in the age of information. In Kirstie Ball, Kevin Haggerty, & David Lyon (Eds.), *Routledge Handbook of Surveillance Studies* (pp. 176-185). Routledge.

West, Robin (2010). Sex, law and consent. In Alan Wertheimer & William Miller (Eds.), *The ethics of consent: Theory and practice* (pp.221-250). Oxford University Press.

Zuboff, Shoshana (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power.* Profile Books.

Acknowledgements

The authors would like to thank Kalyani Menon Sen, an anonymous peer reviewer, their colleagues at the Internet Democracy Project, and all participants at the first virtual Data Governance Network roundtable, held on 24 March, 2020, for their valuable inputs and comments.

About the Authors

Dr. Anja Kovacs directs the Internet Democracy Project in Delhi, India. The Project works towards realising feminist visions of the digital in society, by exploring and addressing power imbalances in the areas of norms, governance and infrastructure in India and beyond. Anja's research and advocacy currently focuses on questions regarding data governance, surveillance and cybersecurity, and regarding freedom of expression - including work on gender, bodies, surveillance, and dataveillance, and gender and online abuse. She has also conducted extensive research on the architecture of Internet governance.

Tripti Jain is a researcher at the Internet Democracy Project for the Bodies and Data Governance Project. Her responsibilities include planning, conducting, and presenting research. Prior to joining the Internet Democracy Project, Tripti was a counsel at Sflc.in. She was managing their Internet Shutdowns project and was involved in various projects that included research and advocacy on issues such as privacy, snd civil rights on the Internet. Tripti is a lawyer by education.

datagovernance.org dgn@idfcinstitute.org

@datagovnetwork /datagovnetwork /datagovnetwork