

Theilen, Jens T. et al.

Article

Feminist data protection: An introduction

Internet Policy Review

Provided in Cooperation with:

Alexander von Humboldt Institute for Internet and Society (HIIG), Berlin

Suggested Citation: Theilen, Jens T. et al. (2021) : Feminist data protection: An introduction, Internet Policy Review, ISSN 2197-6775, Alexander von Humboldt Institute for Internet and Society, Berlin, Vol. 10, Iss. 4, pp. 1-26,
<https://doi.org/10.14763/2021.4.1609>

This Version is available at:

<https://hdl.handle.net/10419/250391>

Standard-Nutzungsbedingungen:

Die Dokumente auf EconStor dürfen zu eigenen wissenschaftlichen Zwecken und zum Privatgebrauch gespeichert und kopiert werden.

Sie dürfen die Dokumente nicht für öffentliche oder kommerzielle Zwecke vervielfältigen, öffentlich ausstellen, öffentlich zugänglich machen, vertreiben oder anderweitig nutzen.

Sofern die Verfasser die Dokumente unter Open-Content-Lizenzen (insbesondere CC-Lizenzen) zur Verfügung gestellt haben sollten, gelten abweichend von diesen Nutzungsbedingungen die in der dort genannten Lizenz gewährten Nutzungsrechte.

Terms of use:

Documents in EconStor may be saved and copied for your personal and scholarly purposes.

You are not to copy documents for public or commercial purposes, to exhibit the documents publicly, to make them publicly available on the internet, or to distribute or otherwise use the documents in public.

If the documents have been made available under an Open Content Licence (especially Creative Commons Licences), you may exercise further usage rights as specified in the indicated licence.



<https://creativecommons.org/licenses/by/3.0/de/legalcode>



SPECIAL
ISSUE



OPEN
ACCESS



PEER
REVIEWED

Feminist data protection: an introduction

Jens T. Theilen *Helmut-Schmidt-University*

Andreas Baur *University of Tübingen*

Felix Bieker *Office of the Data Protection Commissioner Schleswig-Holstein*

Regina Ammicht Quinn *University of Tübingen*

Marit Hansen *Office of the Data Protection Commissioner Schleswig-Holstein*

Gloria González Fuster *Vrije Universiteit Brussel*

DOI: <https://doi.org/10.14763/2021.4.1609>

Published: 7 December 2021

Funding: This work is partially funded by the German Ministry of Education and Research within the project Forum Privacy - Privatheit, Demokratie und Selbstbestimmung im Zeitalter von KI und Globalisierung - PriDS (forum-privatheit.de).

Competing Interests: The author has declared that no competing interests exist that have influenced the text.

Licence: This is an open-access article distributed under the terms of the Creative Commons Attribution 3.0 License (Germany) which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. <https://creativecommons.org/licenses/by/3.0/de/deed.en>
Copyright remains with the author(s).

Citation: Theilen, J. T. & Baur, A. & Bieker, F. & Ammicht Quinn, R. & Hansen, M. & González Fuster, G. (2021). Feminist data protection: an introduction. *Internet Policy Review*, 10(4). <https://doi.org/10.14763/2021.4.1609>

Keywords: Data protection, Privacy, Feminist data protection, Feminism

Abstract: ‘Feminist data protection’ is not an established term or field of study: data protection discourse is dominated by doctrinal legal and economic positions, and feminist perspectives are few and far between. This editorial introduction summarises a number of recent interventions in the broader fields of data sciences and surveillance studies, then turns to data protection itself and considers how it might be understood, critiqued and possibly reimaged in feminist terms. Finally, the authors return to ‘feminist data protection’ and the different directions in which it might be further developed—as a feminist approach to data protection, as the protection of feminist data, and as a feminist way of protecting data—and provide an overview of the papers included in the present special issue.

Introduction: distinguishing privacy and data protection

‘Feminist data protection’ is not an established term or field of study: data protection discourse is dominated by doctrinal legal and economic positions, and feminist perspectives are few and far between. The marginalisation of feminist voices within mainstream discourse, in and of itself, is common enough to not be surprising (see Charlesworth, 2011, p. 17). Nonetheless, the relative lack of feminist engagement with data protection strikes as somewhat curious in light of the manifold feminist debates surrounding a closely related concept: privacy.

The notion of privacy has been subject to extensive feminist critique and exploration, especially insofar as it concerns the gendered division between private and public spheres and its deconstruction (Allen, 1988; MacKinnon, 1989; Hurtado, 1989; Bhattacharjee, 1996; Scott and Keates, 2004; DeCew, 2015; Weinberg, 2017). Many writers have noted, in particular, the instrumentalisation of privacy to protect the perpetrators of domestic violence (Kelly, 2003). The feminist critique of privacy is, at this point, well-known enough to have entered mainstream debates: it was evoked, for instance, in the 2017 landmark judgment of the Indian Supreme Court, which recognised the existence of a constitutionally protected right to privacy in India.¹ The judgment noted in this sense that ‘[m]any writers on feminism express concern over the use of privacy as a veneer for patriarchal domination and abuse of women’, but stressed that, nonetheless, ‘women have an inviolable interest in privacy’, privacy being ‘the ultimate guarantee against violations caused by programmes not unknown to history, such as state imposed sterilization programmes or mandatory state imposed drug testing for women’ (§ 140 (d)).

This duality of privacy has also been highlighted by many feminist authors (e.g. Allen, 1988, 2011; Squires, 2018; Wischermann, 2003; Klaus and Drüeke, 2008).² It is reflected in several recent developments which indicate an incipient, albeit of-

1. *Justice K.S. Puttaswamy vs. Union of India*, 24 August 2017.

2. Another example is Anita Allen and Erian Mack’s influential claim that the right to privacy is ‘the brainchild of nineteenth-century men of privilege, and it shows’ (Allen and Mack, 1990: 441). Allen and Mack grounded such claim on a critical reading of the seminal article ‘The Right to Privacy’, by Samuel Warren and Louis Brandeis (1980), indeed two nineteenth-century men of privilege. That article did however refer, even if only in a footnote, to a case with implications for a feminist defence of privacy: the case of Marion Manola, a Broadway comedian who had won a case in 1890 against a photographer and the manager of her theatre company. Manola contested their right to make money out of a portrait of her in tights that they had taken surreptitiously, without her consent. She was only one of several women who at the time started to use the law – and more particularly privacy claims – to defend their right to live their lives as ‘modern women’ without being exploited by men (Lake 2016).

tentimes timid, awareness of the need to look at privacy (and data protection) *differently*. In this context one might mention the work on gender-based violations of privacy carried out by the United Nations Special Rapporteur on the Right to Privacy (2020), or work by NGOs such as Privacy International (2018), among others (e.g. Chair, 2020). Historians of privacy have been exploring past connections between feminism, liberation and privacy (Igo, 2018), and American scholars keep active exploring privacy's potential to counter the oppression of women, queer folks, and racial and religious minorities (Skinner-Thompson, 2020).

Privacy and data protection are often viewed in tandem (Solove, 2002, pp. 1109-1115; Whitman, 2004, pp. 1189-1195; ECJ, Schecke, and Eifert, 2010). Perhaps this relation accounts, in part, for the relative lack of feminist engagement with data protection: a feminist critique of data protection could perhaps be viewed as unnecessary because privacy has already been dealt with at length from such perspective, and the two concepts are too entwined for data protection to be considered worthy of separate debates. However, for all their areas of overlap, privacy and data protection should not be conflated (Bieker, forthcoming; Cohen, 2019, p. 23; González Fuster, 2014a). They have separate genealogies (González Fuster, 2014b) that have generated differing approaches, connotations and debates in various contexts. Data protection may serve interests other than privacy,³ and it may be better or less well suited at responding to different kinds of potential harms based on how it has been conceptualised thus far, or could be conceptualised in the future. Against this backdrop, we ask: what potential does feminism hold for data protection, and what potential does data protection hold for feminism?

We note at the outset that we approach these questions based on a broad understanding of feminism. Questions of gender are, of course, central to feminist analysis, but gender itself is 'embedded in a range of social, political, cultural, and ideological formations', as Angela Davis has put it. Feminism, therefore, 'involves so much more than gender' (2016, chapter 8; see also Butler 2007, pp. 4-5 and, in the context of data feminisms, D'Ignazio and Klein, 2020, p. 14). It is impossible, in other words, to tackle questions of gender, sexism and patriarchy without simultaneously accounting for other forms of oppression such as racism, (neo-)colonialism, capitalism, etc.⁴ To disregard these in favour of an ostensibly universal notion

3. The General Data Protection Regulation (GDPR), for instance, is a key element of European Union (EU) data protection law. It explicitly serves all fundamental rights and particularly the fundamental right to personal data protection.

4. We use the "etc." here not to demote other forms of oppression to relative insignificance, but to signal that any attempt to list them would, as Butler (2007, p. 196) puts it, "invariably fail to be com-

of womanhood or sisterhood (see critically Mohanty, 2006) is to disregard how various oppressive structures interact and, collectively, impact differently upon different women and gender non-conforming people (Combahee River Collective, 1977; hooks, 1981; Davis, 1983; Collins, 1990; Lorde, 2007; Crenshaw, 1989, 1991; Collins and Bilge, 2020).

How might we place feminism, thus understood, in relation to data protection? We begin by summarising a number of recent interventions in the broader fields of data sciences and surveillance studies which, although they do not usually refer explicitly to the notion of data protection, can teach us about the kind of themes and questions that are important from a feminist perspective. We then turn back to data protection itself and consider how it might be understood, critiqued and possibly reimagined in feminist terms. Finally, we return to the term ‘feminist data protection’ and the different directions in which it might be further developed—as a feminist approach to data protection, as the protection of feminist data, and as a feminist way of protecting data—and we provide an overview of the papers included in the present special issue on feminist data protection.

Feminist surveillance studies and data feminisms

The feminist writings on themes of privacy, surveillance and data processing already constitute a veritable feminist archive.⁵ It is impossible to do justice to their depth, breadth, and variety here—all the more so since feminism employs a broad range of perspectives and methods (Abu-Laban, 2015, p. 45; see generally Vergès, 2021, pp. 19-20), often emphasising embodied, situated and contextual knowledge (Koskela, 2012, p. 50; Costanza-Chock, 2018; D’Ignazio and Klein 2020, p. 83). It is also difficult and delicate to trace a firm line between writings about surveillance, privacy and data protection and works on the rights of women online, including on online harassment and gender-based violence, which have a direct connection with privacy (Citron, 2014; Goldberg, 2019)—and which would equally deserve detailed discussion. Here, we merely hope to sketch some broad lines and distil some common themes to provide an impression of the kind of work that could inspire (or form part of) feminist data protection.

plete”; in this sense, the “illimitable et cetera [...] offers itself as a new departure for feminist political theorizing”.

5. See generally Ahmed 2017, p. 17: “The materials are books, yes, but they are also spaces of encounter; how we are touched by things; how we touch things. I think of feminism as a fragile archive, a body assembled from shattering, from splattering, an archive whose fragility gives us responsibility: to take care”.

Doing critical research and explicitly taking a feminist stance almost inevitably means questioning the status quo—things as they currently stand—and thus also questioning the objectivity in which the status quo commonly dresses itself: it is about ‘wishing, hoping, aiming at everything that has been deemed impossible’ (Olufemi, 2020, p. 1). This involves challenging the objectivity of certain modes of governance, the alleged objectivity of technology, and the techno-determinism and lack of accountability which come with it (Benjamin, 2019, pp. 40-41, 53; see also Magnet, 2011; Nkonde, 2019-2020, p. 32). Connections can be drawn, for example, to big data myths that ‘bigger data are considered somehow more true’—which has ‘close ties with the spectre of objectivity so well-known to feminist critics of knowledge production’ (Shephard, 2016, p. 4; see also boyd and Crawford, 2012).

Rather than being seen as objective, the various forms of technology, surveillance and data processing must be regarded in light of their social origins and contexts (Corones and Hardy, 2009, p. 388; Haggerty and Ericson, 2000; Zuboff, 2015, p. 75). Technology is embedded in social relations (see e.g. Bijker and Law, 1992), in a relationship that can be understood as co-constitutive (e.g. Latour, 2005). Accordingly, it should come as no surprise that technology, surveillance and data processing reproduce, entrench and deepen various forms of discrimination, marginalisation and oppression already present in society (see for instance Gilliom, 2001). A particular form of discrimination and marginalisation is sometimes captured as ‘bias’ within data systems. ‘Bias’ can be a useful framing to draw attention to discriminatory effects, but it can also be a reductive term, since it may signal the possibility of an easy fix by diversifying the underlying data set or the team behind it—which in many cases falls short of a just or even, for some, a liveable solution. For example, while diversification of fields such as machine learning is sorely needed (World Economic Forum, 2018), diversity will not realistically, by itself, achieve the upheaval of these fields’ structures of marginalisation and exclusion. Behind a pleasant rhetoric of diversity there often lurks the tokenisation and gaslighting of those from marginalised groups, especially women of colour (Birhane and Guest, 2021, pp. 65-68; Benjamin, 2019, pp. 19-20, pp. 61-62; Hassan, 2018; see generally Ahmed, 2012).

The discriminating impact of data processing is not exclusively connected to biased input and training data; social sorting and discrimination are its inherent effects (Gandy, 2010; Lyon, 2003). Computer-assisted decision-making might be less prone to individual biases, yet it ‘may also normalize the far more massive impacts of system-level biases’ and ignorance with respect to structural disadvantages (Gandy, 2010, p. 33). Guzik (2009, p. 12) claims that ‘predictive data mining dis-

criminate by design' since its main aim is to distinguish groups and to sort individuals into them (see also Taylor, 2017, p. 15). These groups are the foundation for decisions, e.g. about which users get to see which advertisement, which group will be subject to further security checks and more. Data from one individual might lead to conclusions that affect all members of an artificially created group. The effect of individuals being sorted following their individual data into groups, leading to group categorisations that become the basis of how individuals are treated, might be called statistical discrimination (Guzik, 2009). Since the group and collective aspect of personal data processing becomes more important in big data and machine learning environments, scholars began to increasingly focus on group and collective aspects of data protection beyond the individual (e.g., Matzner, 2014; Mantelero, 2016; Taylor, Floridi, and van der Sloot, 2017).

The idea that data bias can be countered by the diversification of underlying data sets, while apposite in some contexts, can also distract from the fact that certain technologies should, from a feminist standpoint, be opposed entirely rather than merely being made more inclusive and accurate (Powles and Nissenbaum, 2018). The field of facial recognition and its various offspring and connected practices, such as automated gender recognition, is one such case. Feminist scholars have long since exposed the inaccuracies (or, more precisely, the variable degree of accuracy) of facial detection and facial recognition along the lines of race, gender and their intersections (Buolamwini and Gebru, 2018) as well as the binary and cisnormative assumptions of gender it employs (Keyes, 2019; see also Costanza-Chock, 2018). In light of the way these technologies are used by the carceral state for the surveillance and oppression of marginalised groups, however, fighting for inclusion may prove harmful rather than emancipatory (Kalluri, 2020; Keyes, 2019; Hassein, 2017).

Inequality, in brief, should often not be seen as a minor deviation within data processing practices and machine learning, but rather as constitutive of the field and hence not amenable to a technical fix (Fourcade and Johns, 2020, p. 827): 'sexism is a feature, not a bug' (Hicks, 2021). Surveillance and data processing have historically been used as tools of patriarchy, slavery and colonialism as well as for the regulation and oppression of queer people (Browne, 2015; Foucault, 1977; see also e.g., Khan, 2017; Mason and Magnet, 2012, p. 106; Shephard, 2016, p. 3 and pp. 6-8; Conrad, 2009, p. 384). They should thus be viewed as rooted in these historical practices rather than focussing on some shadows of a specific shiny, new technology which is supposed to otherwise magically fix societal problems. A decolonial feminist lens helps to bring these issues to the fore with particular clarity,

highlighting for example the continuing logics of data extraction from the Global South while creating additional dependencies on corporations from the Global North (Milan and Trere, 2019, pp. 326–327; Couldry and Mejias, 2019, p. 6; Birhane, 2020; Cohen, 2018, p. 221), and the pernicious narratives of data for development or surveillance humanitarianism (see Pendergrast, 2019).

A further issue of particular interest from a feminist perspective is the normativity and normalising tendency of categorisation within data processes (Ball et al., 2009, p. 354; D'Ignazio and Klein, 2020, p. 100). We can ask not only which subjects are included in certain data processes or technologies and on which terms, but also how gendered and racialised subjecthood is constituted and essentialised in these contexts in the first place (Browne, 2015, p. 114; Hicks, 2019, pp. 26 and 29; Keyes, 2019; Beauchamp, 2019, p. 15). And again, this is not only true for the modern iterations of classifications such as the gender 'options' on Facebook (Bivens, 2017), but also for other data practices (see Hicks, 2019) such as the development of driver's licenses not just as means of identification but as a way of 'consolidating racial, gender and ability categories into population-level typologies and hierarchies' (Adair, 2019, p. 585).

To focus on subjecthood also raises the question of who is seen as subject and who is objectified—within surveillance and data processing practices, who collects data and whose data is collected, who is acting and who is acted upon, who is watching and who is being watched (Koskela, 2012, p. 51; Andrejevic, 2014; Abu-Laban, 2015, p. 46; Gurumurthy and Chami, 2016)? Women and other marginalised groups have long been familiar with the 'male gaze' which may not only lead to self-regulation and behavioural modification by virtue of the constant feeling of being watched (Khan, 2017), but can also be understood as 'visually dismembering and reconstituting women's bodies' (Mason and Magnet, 2012, p. 107). The 'white gaze' similarly involves the 'imposition of race on the body' (Browne, 2015, p. 7).⁶

Not only the likelihood, but also the consequences of being watched can differ greatly. The narrative that 'those who have nothing to hide have nothing to fear' disregards the way in which surveillance erodes democratic structures in general, but also fails to account for the uneven distribution of how much can safely be revealed along lines of gender, race, class, residency status, occupation and other

6. Browne and others have described this process, in particular, by reference to Frantz Fanon's 'Look, a Negro!' passage in *Black Skin, White Masks* (2008, ch. 5). As Ruha Benjamin notes (2019, p. 124), it echoes eerily in the work of Joy Buolamwini (2016) on the 'coded gaze', as she had to don a literal white mask for facial recognition technology to recognise her face. A further example of work on the 'gaze' is Dan Kotliar's discussion (2020) of the continuities and ruptures between the 'colonial gaze' and the 'algorithmic gaze'.

factors (Shephard, 2016, p. 13). We might think, for example, of data processing leading to the possibility of stalking and sexual harassment of women (Mason and Magnet, 2012), to tracking of pregnancy and abortion or to being outed as queer or as a sex worker (Kovacs, 2020). Furthermore, under neoliberal capitalism practices of self-tracking are becoming more common—and the example of menstrual apps clearly demonstrates the extent to which this can involve the unwaged labour of women and others who menstruate (McEwen, 2018).

In sum, feminist interventions in the fields of surveillance, data processing and machine learning invite us to ask different questions than those that otherwise dominate research agendas. In particular, they invite us to ask uncomfortable questions about power structures and the ways in which they are gendered, raced and classed (Kalluri, 2020; D'Ignazio and Klein, 2020, ch. 1)—and to investigate how they have been and can continue to be opposed and dismantled (Costanza-Chock, 2018). Whatever the dangers involved, where there is surveillance, there is subversion and parody to undermine it, and where there is a white, male gaze, there is also an oppositional gaze (Browne, 2015, pp. 10 and 58, building on hooks, 1992).

Data processing, data protection and feminist critique

While feminist interventions have analysed the dynamics of data processing and the dangerous outcomes such processing can produce, they have rarely engaged explicitly with data protection (but see e.g., Peña and Varon, 2019; Suárez-Gonzalo, 2019). A preliminary issue is how data protection should itself be understood: reference is often made to the European legal context and particularly to the General Data Protection Regulation (GDPR; see Daly, 2021, p. 67), but even so data protection has been construed in many different and sometimes contradictory ways (Bieker, forthcoming; Hustinx, 2017; Tzanou, 2017; Lynskey, 2015; Docksey, 2015; Kokott and Sobotta, 2014; Kranenborg, 2014; Purtova, 2012; Rouvroy and Poullet, 2009; De Hert and Gutwirth, 2006).

One way of approaching the notion of data protection is to go back to its origins. The discourse on data protection in Europe started in the 1960s with the introduction of data processing in the public service—already then with a marked international dimension, building on parallel reflections on the other side of the Atlantic regarding what the United States would eventually conceptualise as ‘informational privacy’. When the German state Hesse set out to employ large databases for public information systems, it also enacted the first legislation to use the term ‘data protection’ (González Fuster, 2014a, p. 56), the *Datenschutzgesetz* of 1970. A report prepared for the German Ministry of the Interior concerning the foundations of da-

ta protection and its future development shines some light on how data protection was understood at the time: it was viewed as a necessary companion of data processing due to the inherent power asymmetry between those who process and control the data and those whose data are processed (Steinmüller et al., 1972, p. 40ff). The report recognised that data processing may have adverse effects both on individuals and on society as a whole, and was therefore viewed as encompassing both individual and structural dimensions (Steinmüller et al., 1972, pp. 34 and 44; see Bieker, forthcoming). It is also noteworthy that even at this early stage of discussion, data protection was considered a necessary safeguard to protect minorities in particular, as they could easily be discriminated against with the use of data processing technology (Steinmüller et al., 1972, p. 40).

Elements of these early conceptualisations continue to play a role in current debates on data protection—in particular, data protection is still conceptualised by some authors as a response to the power imbalance that lies at the heart of data processing (Bieker, forthcoming; Lynskey, 2015, p. 105; Malgieri and Niklas, 2020, p. 2; Rouvroy and Poullet, 2009, p. 68 and pp. 73–74). While there is no agreement on how to remedy, mitigate or transform this power imbalance, the notion of ‘data protection as a critique of power’ (Bergemann, 2018, p. 126) makes it a potential ally of the various feminist perspectives discussed above. In this sense, data feminism, according to the principles formulated by Catherine D’Ignazio and Lauren Klein, ‘begins by analyzing how power operates in the world’ and ‘commits to challenging unequal power structures and working toward justice’ (2020, p. 17).

If understood as a critique of power, then, there is clearly some measure of affinity between data feminisms and data protection. However, as noted above, understandings of data protection are not uniform or consistent. As so often, dominant understandings—particularly those prevalent within legal discourse—tend to shift the focus away from challenging power structures and instead offer merely individualistic, liberal frameworks which largely serve to preserve and legitimise the status quo (Padden and Öjehag-Pettersson, 2021, p. 13; Bergemann, 2018, p. 127). The conventions of legal discourse also bring assumptions of objectivity and rationality with them which, as feminist and other critical approaches to law have long since pointed out (MacKinnon, 1983; Charlesworth, Chinkin, and Wright, 1991; Kennedy, 1997; Theilen, 2021), serve to mask the gendered power structures of which law forms part—in a very similar way to the alleged objectivity of technology mentioned above. Against this backdrop, it becomes important to offer a feminist critique of data protection by centring categories such as gender, race and class, but also more generally by applying feminist insights on the analysis of un-

equal power structures to those involved in data processing (Peña and Varon, 2019; Suárez-Gonzalo, 2019, p. 184).

We might ask, for example, who the subject behind data protection is (Malgieri and González Fuster, 2021). In legal terms, the ‘data subject’ is defined simply as an ‘identified or identifiable natural person’ (Article 4(1) GDPR). It is thus assumed to exist as a pre-constituted subject, thereby side-lining the above-mentioned questions of how subjecthood is constituted in the first place and the conditions and gendered power structures which shape it (see critically, Cohen, 2019), for example the way in which self-tracking may involve digital reproductive labour which produces both data and subjectivities (McEwen, 2018, p. 246). By positing a data subject ostensibly ‘unmarked’ by notions such as gender, race, and class (see generally Frankenburg, 1993), it also becomes difficult to respond appropriately to the way in which surveillance and data processing specifically target women and other marginalised groups, as described above. It would therefore be necessary, at a minimum, to ‘emphasise existing inequalities between different data subjects and specify in a more systematic and consolidated way that the exercise of data rights is conditioned by many factors such as health, age, gender or social status’ (Malgieri and Niklas, 2020, p. 2).

One area in which these questions of subjecthood become particularly tangible is the question of consent. Feminist theory and praxis has a complicated relation to the notion of consent, both highlighting its importance (‘no means no’) and offering trenchant critiques of its limitations. In that vein, for example, it has been argued that commonplace understandings of consent unrealistically presuppose a free, liberal subject capable of making a meaningful choice (see Hirschmann, 1992; Drakopoulou, 2007) and that foregrounding consent therefore fails to account for—and hence legitimates—gendered power structures which shape the situation in which consent can be given (Lacey, 1998; MacKinnon, 1989; Pateman, 1988; Loick, 2019).

The same argumentative structure can be transferred to critiques of data protection: when focussing on consent to data processing, we easily lose sight of the way in which the situation of consent-giving is itself shaped by the more general power imbalance between data subject and controller (see generally Peña and Varon, 2019, pp. 13-14; Suárez-Gonzalo, 2019, p. 184; Cifor et al., 2019; Bietti, 2020, p. 339; Padden and Öjehag-Pettersson, 2021, pp. 12-13; de Hingh 2018, pp. 1279-1281; Bergemann, 2018, p. 113). As necessary a safeguard as consent may be in certain situations, then, it also constitutes another way in which data protection is diverted away from truly challenging the unequal power structures inherent in

data processing. This goes both for the capitalist logics of data extraction underlying large-scale data processing (Andrejevic, 2014, p. 1675) and for the gendered and racialised foundations of surveillance.

These dynamics are not necessarily specific to the notion of consent, however—a fact which is important to note since, at least from a European legal perspective, consent constitutes only one possible legal base for data processing (see Art. 6 GDPR) and thus plays a less central role within data protection than is sometimes assumed. Other bases for data processing, too, can be questioned from a feminist perspective: for example, in light of the insights from data feminisms canvassed above, it seems immediately clear that interpretations of the ‘public interest’ will involve preconceptions about which persons or groups should be subject to regulation and surveillance.

Within the current legal data protection framework, it can be regarded as difficult to effectively challenge not only individual acts of data processing but rather the discrimination against groups and collectives, as well as certain technologies, business models or mass surveillance practices altogether (see Daly, 2021, p. 88; Rule, 2012, pp. 67–68). Take the example of artificial intelligence (AI). Early conceptualisations of data protection included a prohibition of hyper-complex processing operations: if they were so expansive or complicated that a controller could not describe their necessity comprehensively, they would not be allowed (Podlech, 1982, p. 456). Today, hyper-complex processing operations *could* still be understood as violating various rules and principles of data protection law (Bieker, forthcoming); however, the express formulation of a prohibition did not find its way into written law, and the GDPR is not commonly read as containing such a prohibition. Instead, the legislator takes a sectoral approach to certain technologies. Even the current proposal for an EU regulation on AI (EU Commission, 2021), which includes a prohibition of certain AI practices, only rules out a very limited number of applications and includes, tellingly, exceptions for law enforcement.

As mentioned above, there is a risk that notions like transparency, fairness or accuracy, which play a prominent role in liberal data protection discourse (Maxwell, 2015), may function merely as a distraction from more foundational feminist concerns about the way technologies such as automated gender recognition both entrench cisnormative views of gender as ‘readable’, normalise mass surveillance along gendered and racialised lines, and expand the reach of the carceral state at the expense of already oppressed groups. At least in the legal conceptualisation of data protection, such practices will largely continue to be legitimated by reference to the public security interest (Bigo, 2012, p. 277; see e.g. ECJ, Digital Rights Ire-

land, 2014, paras. 41-42; ECJ, *La Quadrature du Net and others*, 2020)—which in turn is based on perceptions of risk that are strongly shaped by notions such as gender, race and class (see Stachowitsch and Sachseder, 2019; Beauchamp, 2019; Costanza-Chock, 2018; Currah and Mulqueen, 2011).

Since data protection, as it is commonly understood, is so strongly tied up with the European legal order, aspects of this integration process place limitations on it in several ways. The project of European integration is not as simple as often portrayed and many scholars offered understandings and conceptualisations of this process beyond the discourse of liberalism, human rights and peace (see e.g. Bigo et al., 2021; Wiener et al., 2018). One aspect is that the preservation of colonial power structures played a considerable role in European integration (Garavini, 2012; Hansen and Jonsson, 2015). This stands in contrast to decolonial feminism, which would aim to direct the critical potential of data protection towards challenging data extraction from the Global South, rather than re-consolidating European values as universal (see Arora, 2019, p. 718). Given that one of the main aims of the European Union is to establish a free market, and the EU is thus wedded to (neo)liberalism and capitalism (O'Connell, 2019), why would we expect it to move beyond a capitalist (Daly, 2021, pp. 88 and 92), individualised approach to data protection and instead centre projects of collective resistance (Suárez-Gonzalo, 2019, p. 184; Hull, 2015, p. 98; Arora, 2019) or communal, non-commodifying data practices, as feminist voices would demand?⁷ Of course, data protection could be (re-)imagined in many different ways, some of them with more emancipatory force than others. In reckoning with its dominant conceptualisations, however, we need to be aware that they are developed 'within a context that includes systematic constraints and pressures' (Marks, 2009, p. 2)—and that these constraints limit the feminist potential of data protection as a critique of power.

Outlook: where could we take 'feminist data protection'?

We noted at the outset that 'feminist data protection' is not an established term or field of study—not yet. The picture sketched above perhaps points towards a further reason for the relative lack of feminist engagement with data protection: as a

7. See, for example, the Feminist Data Manifest-No (Cifor et al., 2019), which reads in part: 'We commit to taking back control over the ways we behave, live, and engage with data and its technologies. [...] We commit to centering creative and collective forms of life, living, and worldmaking that exceed the neoliberal logics and resist the market-driven forces to commodify human experience. [...] We refuse work *about* minoritized people. We commit to mobilizing data so that we are working with and for minoritized people in ways that are consensual, reciprocal, and that understand data as always co-constituted'.

term strongly associated with European legal doctrine and thus also linked to neo-liberal, capitalist logics it might seem to hold little interest for feminist endeavours of social transformation.⁸ Indeed, although data protection has been and can be conceptualised as a response to the asymmetric power structures inherent in data processing, its radical potential is limited by the way those very power structures fade into the background within individualistic, law-based approaches which dominate mainstream debates. Against this backdrop, we would like to suggest three complementary ways of understanding ‘feminist data protection’, each of which points towards different forms of analysis and offers different possibilities and prospects.

The *first understanding* is the one we have been foregrounding thus far: feminist data protection can be understood as a feminist critique of data protection, or as *doing and thinking data protection from a feminist perspective*. With this understanding, ‘feminist’ is an attribute of ‘data protection’.

This approach brings certain questions, topics and interests into the established field of data protection, and challenges its mainstream methods by looking at structural inequalities and power imbalances, questioning presuppositions of order, fixed categories, normality and objectivity, and examining the possibilities of re-establishing data protection as a field for social transformation. We have noted some ways in which the historical origins of data protection as well as some current debates hold potential in that regard, but also identified some limitations. To acknowledge the latter does not imply that we should disengage from data protection entirely, or position ourselves as unproblematically ‘against’ it. To do so would be to cede even more space to those whose power is, however imperfectly, constrained by current regulations: this becomes clear, for example, in the resistance by certain states to the EU’s stance on both data protection issues and gender equality.⁹ It does mean, however, that we should be wary of where we place our hopes for social transformation, and that we should not let established liberal discourses on data protection delimit our transformative horizons.

A concrete example of this type of potentially transformative feminist theory and practice ‘of data protection’ is the interrogation of online gender construction via

8. For arguments explaining why EU data protection law has historically not focused on the question of data protection *for whom*: Tzanou, 2020.

9. For example, the United Kingdom started discussing the possibility of reducing its data protection safeguards very soon after it left the EU, while at the same time Poland was putting gender at the centre of its frictions with the EU, e.g. by refusing to back up a Council declaration on human rights and AI if it mentioned ‘gender’ (Stolton, 2020).

data protection law, and notably through the exercise of data subject rights.¹⁰ This implies, in particular, investigating data protection transparency obligations and data subject rights to see how they can be further used to apprehend, and eventually contest and play with, the ways in which gender is attributed online—on the understanding that not only gender but many other categorisations would benefit from this unmasking and interrogation.

The two further understandings of ‘feminist data protection’ we propose, approach the task of thinking beyond established discourses on data protection by building bridges to the various data feminisms canvassed above, which do not necessarily make use of the concept of data protection, or at least aim to radically rethink its connotations. The *second understanding* of feminist data protection positions ‘*feminist*’ as an attribute of ‘*data*’, rather than ‘data protection’: it is thus concerned with *the protection of feminist data*.

Of course, if one thinks of data simply as ‘given’ (literally, the ‘datum’), then there might not be feminist data. However, this understanding of data is simplistic: there is no ‘raw data’ (Gitelman, 2013; Pendergrast, 2019). We must reflect critically on which information needs to become data before it can be trusted, and whose experiences need to become data before they can be considered as ‘fact’ and acted upon (see Williams, 1995, p. 47; Collins, 2019, chapter 4), which involves tackling the structural marginalisation of women, especially women of colour, beyond mere references to ‘diversity’. Data sciences are increasingly becoming subject to feminist critique along these lines (D’Ignazio and Klein, 2020), and scholars and activists are aiming to develop feminist data sets including art work, literature, interviews, narratives, political writing and much more.¹¹ The protection of feminist data would involve the presence, recognition and the just and democratic handling of these data in common knowledge and consciousness, in politics and activism, in sciences, and in tools like statistical modelling, data visualisation, and crowd-sourcing. It is particularly crucial in contexts in which data concerning feminist resistance places individuals and groups at risk, but in which notions like privacy do not seem useful since visibility is inextricably tied up with resistance to patriarchal structures (see Arora, 2019).

10. See, for example: Gloria González Fuster, *FAT* 2020 Invited Tutorial ‘Gender: What the GDPR does not tell us (But maybe you can?)’*, <https://fat2020-tutorials.github.io/gender-gdpr/>. On the opacity of gender categorisation online, see also: Fosch-Villaronga et al., 2021.

11. A ‘feminist data set’ is currently being developed, for example, as part of a multi-year project by Caroline Sindors (2020); for further examples of initiatives working on data justice, some of which involve feminist data sets, see Costanza-Chock, 2018.

The *third understanding* of ‘feminist data protection’, finally, takes ‘feminist’ to be an attribute of ‘protection’: it refers, in other words, to a *feminist way of protecting data*, which involves questioning what it means to ‘protect data’ in the first place.

A first question might be whether ‘protecting data’ is actually about protecting something, as the phrasing of ‘data protection’ would have it, or about protecting someone: debates about the potentially conflicting aims of European data protection law (enabling inter-state data flows and protecting data subjects) point in this direction (see Padden and Öjehag-Pettersson, 2021; Daly, 2021, pp. 87–88). But this would only be a starting point: if protecting data is about protecting some-body, then whose body is it and what are the relations between these individuals, their data, their bodies and society at large? What would it mean to centre the body in our analyses of data processes (see Conrad, 2009; van der Ploeg, 2012; Cifor et al., 2019; Kovacs, 2020), taking into account its constitution through the white, male gaze as described above? Questions such as these point beyond a stable data subject and towards the analysis of how subjecthood is constituted within data practices and what this might mean from a feminist perspective.

Questioning the notion of ‘protection’ would be another key element of this understanding of feminist data protection. Philosophical, historical, psychological and ethical research has shown that the act of protecting someone is often situated in asymmetrical, often patriarchal relationships of power. At the same time, concepts of ‘care’ structure feminist discourses regarding private as well as public contexts and their entanglements (Graham, 1991; Larrabee, 1993; Engster, 2005; in the context of surveillance see Abu-Laban, 2015). Especially theories and practices of health care and other care work, but also economic and environmental studies have approached different notions of care. However, there remains a gap in reflecting data protection as ‘care work’. A feminist approach to ‘protection’ needs to leave behind the object of protection as ‘object’, instead working towards dialogical intersubjective forms of encounter involving respect, empowerment and care (see Cifor et al., 2019).

All three ways of understanding ‘feminist data protection’ are important, and while they do not exhaust the field of possibilities offered by various data feminisms more broadly, we believe that they offer significant critical potential for challenging the power structures involved in data processing. It is in that spirit that the articles contained in the special issue which this paper introduces deal with a broad range of topics—and from a wide range of disciplines including but not limited to international relations, law, sociology and ethics—under the umbrella of feminist data protection(s).

Aisha Paulina Lami Kadiri approaches the task of re-imagining data protection by offering a trenchant critique of the data subject. Instead of individualised, liberal notions, she proposes to centre an Afrofuturist data subject that is radically subjective, collective and contextual.

Garfield Benjamin analyses and critiques 'data collection' using data feminism and a performative theory of privacy. The contribution discusses the (negative) implications of the term 'data collection' under three main narratives: data as resource, data as discovery and data as assumption. Benjamin concludes by exploring several alternative concepts and suggests using the term 'data compilation' in order to allow for awareness and critique of power relations.

Jenni Hakkarainen argues that algorithmic discrimination is a collective issue and requires collective redress, which the current rules of legal procedure and access to justice do not offer. She finds that *ex ante* oversight mechanisms that allow for action on the collective level can remedy these structural issues, as they allow for an intervention before any violations occur.

Laura Carter focusses on the welfare benefits system in the UK and how it utilises both gender stereotyping and surveillance in ways that harm both individuals and society as a whole. She argues that particular data-based surveillance and gender stereotyping act to reinforce each other, creating a vicious cycle in which the surveilled are incentivised to conform, and the non-conforming are increasingly surveilled.

Joana Varon and Paz Peña offer a feminist and anti-colonial analysis of automated decision-making in social welfare programmes. In particular, they draw parallels between feminist critiques of consent and the role consent plays in digital welfare states in the Global South, arguing that we need a collective approach to consent in order to challenge the systems of oppression at play.

Paola Lopez analyses various examples of structural inequalities and defines three types of bias: technical bias, socio-technical bias and societal bias. She shows the benefit of clearly distinguishing between these different types of bias for scrutinising data-based algorithmic systems.

The contribution of Renee Shelby, Jenna Harb, Kathryn Henne examines digital technologies designed to support survivors of sexual and gender-based violence through an intersectional lens, and shows how these technologies reaffirm normative whiteness. Their message is powerful: feminist conceptualisations of data pro-

tection must confront and dismantle the ways in which whiteness operates as the normative lens for personal data processing.

Anastasia Siapka and Elisabetta Biasin bring the insights of feminist theories of labour and political economy to bear on data sharing in the context of fertility and menstruation tracking apps. They argue that data protection and consumer protection laws are insufficient to alleviate the power balances involved and explore the potential of a demand for wages for digital labour.

Lucy Hall and William Clapton explore how the deployment of technologies programmed to attempt to detect lies and deceit at the borders of the EU will negatively impact those who are already marginalised. In doing so, they illustrate applications of AI that are inherently (cis)gendered, sexualised and racialised.

Finally, Isabelle Bartram, Tino Plümecke and Andrea zur Nieden examine extended DNA analysis, a technology pushed by security policymakers ostensibly to protect white German women from male migrants, invoking racist imaginaries of a “dangerous other”. The authors conclude that the initiative does not deliver on the promises of a “DNA composite sketch” and will increase unacknowledged institutional bias against minorities due to unquestioned trust in this technology.

In sum, all the contributions will open, we hope, new perspectives for feminist data protection(s), and for data protection generally.

References

- Abu-Laban, Y. (2014). Gendering Surveillance Studies: The Empirical and Normative Promise of Feminist Methodology. *Surveillance & Society*, 13(1), 44–56. <https://doi.org/10.24908/ss.v13i1.5163>
- Adair, C. (2019). Licensing Citizenship: Anti-Blackness, Identification Documents, and Transgender Studies. *American Quarterly*, 71(2), 569–594. <https://doi.org/10.1353/aq.2019.0043>
- Ahmed, S. (2012). *On Being Included: Racism and Diversity in Institutional Life*. Duke University Press. <https://doi.org/10.1515/9780822395324>
- Ahmed, S. (2017). *Living a feminist life*. Duke University Press.
- Allen, A. L. (1988). *Uneasy access: Privacy for women in a free society*. Rowman & Littlefield.
- Allen, A. L. (2011). *Unpopular privacy: What must we hide?* Oxford University Press.
- Allen, A. L., & Mack, E. (1990). How privacy got its gender. *Northern Illinois University Law Review*, 10(3), 441–478.
- Andrejevic, M. (2014). The Big Data Divide. *International Journal of Communication*, 8, 17.

Arora, P. (2019). General data protection regulation – A global standard?: Privacy futures, digital activism, and surveillance cultures in the Global South. *Surveillance & Society*, 17(5), 717–725. <https://doi.org/10.24908/ss.v17i5.13307>

Ball, K. S., Phillips, D. J., Green, N., & Koskela, H. (2009). Surveillance Studies needs Gender and Sexuality. *Surveillance & Society*, 6(4), 352–355. <https://doi.org/10.24908/ss.v6i4.3266>

Beauchamp, T. (2019). *Going Stealth: Transgender Politics and U.S. Surveillance Practices*. Duke University Press. <https://doi.org/10.2307/j.ctv11cw8g8>

Benjamin, R. (2019). *Race after technology: Abolitionist tools for the new Jim code*. Polity.

Bergemann, B. (2018). The Consent Paradox: Accounting for the Prominent Role of Consent in Data Protection. In M. Hansen, E. Kosta, I. Nai-Fovino, & S. Fischer-Hübner (Eds.), *Privacy and Identity Management. The Smart Revolution* (Vol. 526, pp. 111–131). Springer International Publishing. https://doi.org/10.1007/978-3-319-92925-5_8

Bhattacharjee, A. (1996). The public/private mirage: Mapping homes and undomesticating violence work in the South Asian Immigrant Community. In M. J. Alexander & C. T. Mohanty (Eds.), *Feminist genealogies, colonial legacies, democratic futures* (pp. 308–329). Routledge.

Bieker, F. (2022). *The right to data protection – Individual and structural dimensions of data protection in EU law*. T.M.C. Asser Press.

Bietti, E. (2020). Consent as a Free Pass: Platform Power and the Limits of the Informational Turn. *Pace Law Review*, 40(1), 310–398.

Bigo, D. (2012). Security, surveillance and democracy. In *Routledge Handbook of Surveillance Studies*. Routledge. https://doi.org/10.4324/9780203814949.ch3_3_b

Bigo, D., Diez, T., Fanoulis, E., Rosamond, B., & Stivachtis, Y. A. (2021). *The Routledge handbook of critical European studies*. <https://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&db=nlabk&AN=2666914>

Bijker, W. E., & Law, J. (Eds.). (1992). *Shaping technology/Building society: Studies in Sociotechnical Change*. MIT Press.

Birhane, A. (2020). Algorithmic Colonization of Africa. *SCRIPT-Ed*, 17(2), 389–409. <https://doi.org/10.2966/scrip.170220.389>

Birhane, A., & Guest, O. (2021). Towards Decolonising Computational Sciences. *Kvinder, Køn & Forskning*, 2, 60–73. <https://doi.org/10.7146/kkf.v29i2.124899>

Bivens, R. (2017). The gender binary will not be deprogrammed: Ten years of coding gender on Facebook. *New Media & Society*, 19(6), 880–898. <https://doi.org/10.1177/1461444815621527>

boyd, danah, & Crawford, K. (2012). CRITICAL QUESTIONS FOR BIG DATA: Provocations for a cultural, technological, and scholarly phenomenon. *Information, Communication & Society*, 15(5), 662–679. <https://doi.org/10.1080/1369118X.2012.678878>

Browne, S. (2015). *Dark Matters: On the Surveillance of Blackness* (p. dup;9780822375302/1). Duke University Press. <https://doi.org/10.1215/9780822375302>

Buolamwini, J. (2016). *The Algorithmic Justice League* [Medium Post]. MIT Media Lab. <https://medium.com/mit-media-lab/the-algorithmic-justice-league-3cc4131c5148>

Buolamwini, J., & Gebru, T. (2018). Gender Shades: Intersectional Accuracy Disparities in

Commercial Gender Classification. *Proceedings of Machine Learning Research*, 81, 1–15. <http://proceedings.mlr.press/v81/buolamwini18a.html>

Butler, J. (2006). *Gender trouble: Feminism and the subversion of identity*. Routledge.

Chair, C. (2020). *My data rights: Feminist reading of the right to privacy and data protection in the age of AI* [Report]. My Data Rights. https://mydatarights.africa/wp-content/uploads/2020/12/mydatarights_policy-paper-2020.pdf

Charlesworth, H. (2011). Talking to ourselves?: Feminist scholarship in international law. In S. Kouva & Z. Pearson (Eds.), *Feminist Perspectives on Contemporary International Law: Between Resistance and Compliance?* (pp. 17–32). Hart Publishing.

Charlesworth, H., Chinkin, C., & Wright, S. (1991). Feminist Approaches to International Law. *American Journal of International Law*, 85(4), 613–645. <https://doi.org/10.2307/2203269>

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

Citron, D. K. (2014). *Hate crimes in cyberspace*. <http://www.dawsonera.com/depp/reader/protected/external/AbstractView/S9780674735613>

Cohen, J. E. (2018). The Biopolitical Public Domain: The Legal Construction of the Surveillance Economy. *Philosophy & Technology*, 31(2), 213–233. <https://doi.org/10.1007/s13347-017-0258-2>

Cohen, J. E. (2019). Turning Privacy Inside Out. *Theoretical Inquiries in Law*, 20(1), 1–31. <https://doi.org/10.1515/til-2019-0002>

Collins, P. H. (1990). *Black feminist thought: Knowledge, consciousness, and the politics of empowerment*. Unwin Hyman.

Collins, P. H., & Bilge, S. (2020). *Intersectionality*. Wiley.

Combahee River Collective. (1977). *The Combahee River Collective Statement*.

Conrad, K. (2009). Surveillance, Gender, and the Virtual Body in the Information Age. *Surveillance & Society*, 6(4), 380–387. <https://doi.org/10.24908/ss.v6i4.3269>

Corones, A., & Hardy, S. (2009). En-Gendered Surveillance: Women on the Edge of a Watched Cervix. *Surveillance & Society*, 6(4), 388–397. <https://doi.org/10.24908/ss.v6i4.3270>

Costanza-Chock, S. (2018). Design Justice, A.I., and Escape from the Matrix of Domination. *Journal of Design and Science*. <https://doi.org/10.21428/96c8d426>

Crenshaw, K. (1989). Demarginalizing the Intersection of Race and Sex: A Black Feminist Critique of Antidiscrimination Doctrine, Feminist Theory and Antiracist Politics. *University of Chicago Legal Forum*, 1989(1), 139–167.

Crenshaw, K. (1991). Mapping the Margins: Intersectionality, Identity Politics, and Violence against Women of Color. *Stanford Law Review*, 43(6), 1241. <https://doi.org/10.2307/1229039>

Currah, P., & Mulqueen, T. (2011). Securitizing gender: Identity, biometrics, and transgender bodies at the airport. *Social Research*, 78(2), 557–582.

Daly, A. (In press). Neo-Liberal Business-As-Usual or Post-Surveillance Capitalism With European Characteristics? The EU's General Data Protection Regulation in a Multi-Polar Internet. In R. Hoyng & G. P. L. Chong (Eds.), *Communication Innovation and Infrastructure: A Critique of the New in a*

Multipolar World. Michigan State University Press.

Davis, A. Y. (1983). *Women, race & class* (1st Vintage Books ed). Vintage Books.

Davis, A. Y. (2016). *Freedom is a constant struggle: Ferguson, Palestine, and the foundations of a movement*. Haymarket Books.

De Hert, P., & Gutwirth, S. (2006). Privacy, data protection and law enforcement: Opacity of the individual and transparency of power. In E. Claes, A. Duff, & S. Gutwirth (Eds.), *Privacy and the Criminal Law* (pp. 61–104). Intersentia. https://works.bepress.com/serge_gutwirth/5/

de Hingh, A. (2018). Some Reflections on Dignity as an Alternative Legal Concept in Data Protection Regulation. *German Law Journal*, 19(5), 1269–1290. <https://doi.org/10.1017/S2071832200023038>

Decew, J. W. (2015). The feminist critique of privacy: Past arguments and new social understandings. In B. Roessler & D. Mokrosinska (Eds.), *Social Dimensions of Privacy* (pp. 85–103). Cambridge University Press. <https://doi.org/10.1017/CBO9781107280557.006>

D'Ignazio, C., & Klein, L. F. (2020). *Data feminism*. The MIT Press.

Docksey, C. (2015). Articles 7 and 8 of the EU Charter: Two distinct fundamental rights. In A. Grosjean, *Enjeux européens et mondiaux de la protection des données personnelles*. Larcier.

Drakopoulou, M. (2007). Feminism and consent: A genealogical inquiry. In R. Hunter & S. Cowan (Eds.), *Choice and consent: Feminist engagements with law and subjectivity* (pp. 9–38). Routledge Cavendish.

Engster, D. (2005). Rethinking Care Theory: The Practice of Caring and the Obligation to Care. *Hypatia*, 20(3), 50–74. <https://doi.org/10.1111/j.1527-2001.2005.tb00486.x>

European Commission. (2021a). *Proposal for a regulation of the European Parliament and of the council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts*. Proposal for a regulation: COM/2021/206 final. [https://ec.europa.eu/transparency/documents-register/detail?ref=COM\(2021\)206&lang=en](https://ec.europa.eu/transparency/documents-register/detail?ref=COM(2021)206&lang=en)

European Commission. (2021b). *Proposal for a regulation of the European Parliament and of the council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts, COM(2021)206 final*. [https://ec.europa.eu/transparency/documents-register/detail?ref=COM\(2021\)206&lang=enor](https://ec.europa.eu/transparency/documents-register/detail?ref=COM(2021)206&lang=enor):

European Court of Justice. (2010). *ECLI:EU:C:2010:662*. <https://curia.europa.eu/juris/document/document.jsf?text=&docid=79001&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=39754304>

European Court of Justice. (2014). *ECLI:EU:C:2014:238*. <https://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=39755021>

European Court of Justice. (2020). *ECLI:EU:C:2020:791*. <https://curia.europa.eu/juris/document/document.jsf?text=&docid=232084&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=39755374>

Fanon, F. (1952). *Black skin, white masks* (1st ed., new ed). Grove Press; Distributed by Publishers Group West.

Fosch-Villaronga, E., Poulsen, A., Søraa, R. A., & Custers, B. H. M. (2021). A little bird told me your

gender: Gender inferences in social media. *Information Processing & Management*, 58(3), 102541. <https://doi.org/10.1016/j.ipm.2021.102541>

Foucault, M. (1977). *Discipline and punish: The birth of the prison* (1st American ed). Pantheon Books.

Fourcade, M., & Johns, F. (2020). Loops, ladders and links: The recursivity of social and machine learning. *Theory and Society*, 49(5–6), 803–832. <https://doi.org/10.1007/s11186-020-09409-x>

Frankenberg, R. (1993). *White women, race matters: The social construction of whiteness*. University of Minnesota Press.

Gandy, O. H. (2010). Engaging rational discrimination: Exploring reasons for placing regulatory constraints on decision support systems. *Ethics and Information Technology*, 12(1), 29–42. <https://doi.org/10.1007/s10676-009-9198-6>

Garavini, G. (2012). *After empires: European integration, decolonization, and the challenge from the global South 1957-1986* (R. R. Nybakken, Trans.). Oxford University Press.

Gilliom, J. (2001). *Overseers of the poor: Surveillance, resistance, and the limits of privacy*. University of Chicago Press.

Gitelman, L. (2013). *“Raw data” is an oxymoron*. The MIT Press. <https://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&db=nlabk&AN=2517806>

Goldberg, C. (2019). *Nobody’s victim: Fighting psychos, stalkers, pervs and trolls*.

González-Fuster, G. (2014a). Fighting for Your Right to What Exactly – The Convolved Case Law of the EU Court of Justice on Privacy and/Or Personal Data Protection. *Birkbeck Law Review*, 2(2), 263–278.

González-Fuster, G. (2014b). *The emergence of personal data protection as a fundamental right of the EU*. Springer.

Graham, H. (1991). The Concept of Caring in Feminist Research: The Case of Domestic Service. *Sociology*, 25(1), 61–78. <https://doi.org/10.1177/0038038591025001004>

Gurumurthy, A., & Chami, N. (2016). Data: The new four-letter word for feminism. *GenderIT.org*. <http://doi.org/https://www.genderit.org/node/4738>

Guzik, K. (2009). Discrimination by design: Predictive data mining as security practice in the United States’ ‘War on Terror.’ *Surveillance & Society*, 7(1), 3–20. <https://doi.org/10.24908/ss.v7i1.3304>

Haggerty, K. D., & Ericson, R. V. (2000). The surveillant assemblage. *British Journal of Sociology*, 51(4), 605–622. <https://doi.org/10.1080/00071310020015280>

Hansen, P., & Jonsson, S. (2015). *Eurafrica: The untold history of European integration and colonialism* (First published in paperback). Bloomsbury Academic.

Hassan, A. (2018). *Different stories are possible: On data, feminism and inclusion* [Medium Post]. Digital Society School. <https://medium.com/digitalsocietyschool/different-stories-are-possible-on-data-feminism-and-inclusion-99ee126bff90>

Hassein, N. (2017, August 15). *Against Black Inclusion in Facial Recognition*. Digital Talking Drum. <https://digitaltalkingdrum.com/2017/08/15/against-black-inclusion-in-facial-recognition/>

Hicks, M. (2019). Hacking the Cis-tem. *IEEE Annals of the History of Computing*, 41(1), 20–33. <https://doi.org/10.1109/MAHC.2019.2897667>

- Hicks, M. (2021). Sexism Is a Feature, Not a Bug. In T. S. Mullaney, B. Peters, M. Hicks, & K. Philip (Eds.), *Your Computer Is on Fire* (pp. 135–158). The MIT Press. <https://doi.org/10.7551/mitpress/10993.003.0011>
- Hirschmann, N. J. (1992). *Rethinking obligation: A feminist method for political theory*. Cornell University Press.
- hooks, bell. (1981). *Ain't I a woman: Black women and feminism* (20. print). South End Press.
- hooks, bell. (2015). *Black looks: Race and representation*. <http://site.ebrary.com/id/10953136>
- Hull, G. (2015). Successful Failure: What Foucault Can Teach Us about Privacy Self-Management in a World of Facebook and Big Data. *Ethics and Information Technology*, 17(2), 89–101. <https://doi.org/10.1007/s10676-015-9363-z>
- Human Rights Council. (2020). *Report of the Special Rapporteur on the right to privacy*. UN General Assembly. <https://undocs.org/en/A/HRC/43/52>
- Hurtado, A. (1989). Relating to privilege: Seduction and rejection in the subordination of White Women and Women of Color. *Signs*, 14(4), 833–855. <https://doi.org/10.1086/494546>
- Hustinx, P. (2017). EU data protection law: The review of directive 95/46/EC and the general data protection regulation. In M. Cremona, *New technologies and EU law* (First edition). Oxford University Press.
- Igo, S. E. (2018). *The known citizen: A history of privacy in modern America*. Harvard University Press.
- Kalluri, P. (2020). Don't ask if artificial intelligence is good or fair, ask how it shifts power. *Nature*, 583(7815), 169–169. <https://doi.org/10.1038/d41586-020-02003-2>
- Kelly, K. A. (2003). *Domestic violence and the politics of privacy*. Cornell University Press.
- Kennedy, D. (1997). *A critique of adjudication: Fin de siècle*. Harvard University Press.
- Keyes, O. (2019). The body instrumental. *Logic*, 9. <https://logicmag.io/nature/the-body-instrumental/>
- Khan, S. (2017, November 21). *Surveillance as a feminist issue*. Privacy International. <https://privacyinternational.org/news-analysis/3376/surveillance-feminist-issue>
- Klaus, E., & Drüeke, R. (2008). Öffentlichkeit und Privatheit: Frauenöffentlichkeiten und feministische Öffentlichkeiten. In R. Becker & B. Kortendiek (Eds.), *Handbuch Frauen- und Geschlechterforschung* (pp. 237–244). VS Verlag für Sozialwissenschaften. https://doi.org/10.1007/978-3-531-91972-0_27
- Kokott, J., & Sobotta, C. (2013). The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR. *International Data Privacy Law*, 3(4), 222–228. <https://doi.org/10.1093/idpl/ipt017>
- Koskela, H. (2012). “You shouldn't wear that body.” In *Routledge Handbook of Surveillance Studies*. Routledge. https://doi.org/10.4324/9780203814949.ch1_2_a
- Kotliar, D. M. (2020). Data orientalism: On the algorithmic construction of the non-Western other. *Theory and Society*, 49(5–6), 919–939. <https://doi.org/10.1007/s11186-020-09404-2>
- Kovacs, A. (2020, May 28). *When our bodies become data, where does that leave us?* Deep Dives. <https://deepdives.in/when-our-bodies-become-data-where-does-that-leave-us-906674f6a969>

- Kranenborg, H. (2014). Article 8. In S. Peers, T. Hervey, J. Kenner, & A. Ward (Eds.), *The EU charter of fundamental rights – A commentary*. Hart Publishing.
- Lacey, N. (1998). *Unspeakable Subjects: Feminist Essays in Legal and Social Theory*. Hart Publishing. <https://doi.org/10.5040/9781472561916>
- Lake, J. (2016). *The face that launched a thousand lawsuits*. Yale University Press.
- Larrabee, M. J. (Ed.). (1993). *An Ethic of care: Feminist and interdisciplinary perspectives*. Routledge.
- Latour, B. (2005). *Reassembling the social: An introduction to actor-network-theory*. Oxford University Press.
- Loick, D. (2020). "... as if it were a thing." A feminist critique of consent. *Constellations*, 27(3), 412–422. <https://doi.org/10.1111/1467-8675.12421>
- Lorde, A. (2007). *Sister outsider: Essays and speeches*. Crossing Press.
- Lynskey, O. (2015). *The foundations of EU data protection law*. <http://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&db=nlabk&AN=1108829>
- Lyon, D. (Ed.). (2003). *Surveillance as social sorting: Privacy, risk, and digital discrimination*. Routledge.
- MacKinnon, C. A. (1983). Feminism, marxism, method, and the state: Toward feminist jurisprudence. *Signs*, 8(4), 635–658. <https://doi.org/10.1086/494000>
- MacKinnon, C. A. (1989). *Toward a feminist theory of the state*. Harvard University Press.
- Magnet, S. A. (2011). Introduction: Imagining Biometric Security. In *When Biometrics Fail* (pp. 1–18). Duke University Press. <https://doi.org/10.1215/9780822394822-001>
- Malgieri, G., & González Fuster, G. (2021). The Vulnerable Data Subject: A Gendered Data Subject? *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.3913249>
- Malgieri, G., & Niklas, J. (2020). Vulnerable data subjects. *Computer Law & Security Review*, 37, 105415. <https://doi.org/10.1016/j.clsr.2020.105415>
- Mantelero, A. (2016). Personal Data for Decisional Purposes in the Age of Analytics: From an Individual to a Collective Dimension of Data Protection. *Computer Law & Security Review*, 32(2), 238–255. <https://doi.org/10.1016/j.clsr.2016.01.014>
- Marks, S. (2009). False Contingency. *Current Legal Problems*, 62(1), 1–21. <https://doi.org/10.1093/clp/62.1.1>
- Mason, C. L., & Magnet, S. (2012). Surveillance Studies and Violence Against Women. *Surveillance & Society*, 10(2), 105–118. <https://doi.org/10.24908/ss.v10i2.4094>
- Matzner, T. (2014). Why privacy is not enough privacy in the context of "Ubiquitous Computing" and "Big Data." *Journal of Information, Communication and Ethics in Society*, 12(2), 93–106. <https://doi.org/10.1108/JICES-08-2013-0030>
- Maxwell, W. J. (2015). Principles-based regulation of personal data: The case of "fair processing." *International Data Privacy Law*, 5, 205–216. <https://doi.org/10.1093/idpl/ipv013>
- McEwen, K. D. (2018). Self-Tracking Practices and Digital (Re)productive Labour. *Philosophy & Technology*, 31(2), 235–251. <https://doi.org/10.1007/s13347-017-0282-2>

- Mejias, U. A., & Couldry, N. (2019). Datafication. *Internet Policy Review*, 8(4). <https://doi.org/10.14763/2019.4.1428>
- Milan, S., & Treré, E. (2019). Big Data from the South(s): Beyond Data Universalism. *Television & New Media*, 20(4), 319–355. <https://doi.org/10.1177/1527476419837739>
- Mohanty, C. T. (2006). *Feminism without borders: Decolonizing theory, practicing solidarity* (Reprint). Zubaan.
- Nkonde, M. (2019). Automated Anit-Blackness: Facial recognition in Brooklyn, New York. *Harvard Kennedy School Journal of African American Policy*, 30–36.
- O'Connell, P. (2019). The constitutional architecture of injustice. In T. Ahmed & E. Fahey, *On Brexit* (pp. 55–63). Edward Elgar Publishing. <https://doi.org/10.4337/9781789903010.00011>
- Olufemi, L. (2020). *Feminism, interrupted: Disrupting power*. Pluto Press.
- Padden, M., & Öjehag-Pettersson, A. (2021). Protected how? Problem representations of risk in the General Data Protection Regulation (GDPR). *Critical Policy Studies*, 1–18. <https://doi.org/10.1080/19460171.2021.1927776>
- Pateman, C. (1988). *The sexual contract*. Stanford University Press.
- Peña, P., & Varon, J. (2019). *Consent to our data bodies: Lessons from feminist theories to enforce data protection*. Association for Progressive Communications. <https://codingrights.org/docs/ConsentToOurDataBodies.pdf>
- Pendergrast, K. (2019, November 25). The next big cheap: Calling data “the new oil” takes its exploitation for granted. *Real Life Magazin*. <https://reallifemag.com/the-next-big-cheap/>
- Ploeg, I. van der. (2012). The body as data in the age of information. In *Routledge Handbook of Surveillance Studies*. Routledge. https://doi.org/10.4324/9780203814949.ch2_2_d
- Podlech, A. (1982). Individualdatenschutz – Systemdatenschutz. In K. Brückner & G. Dalichau (Eds.), *Beiträge zum Sozialrecht – Festgabe für Grüner* (pp. 451–462). R. S. Schulz.
- Powles, J., & Nissenbaum, H. (2018). *The seductive diversion of “Solving” bias in Artificial Intelligence* [Medium Post]. OneZero. <https://onezero.medium.com/the-seductive-diversion-of-solving-bias-in-artificial-intelligence-890df5e5ef53>
- Privacy International. (2018). *From oppression to liberation: Reclaiming the right to privacy* (Gender and Privacy) [Report]. <https://privacyinternational.org/sites/default/files/2018-11/From%20oppression%20to%20liberation-reclaiming%20the%20right%20to%20privacy.pdf>
- Purtova, N. (2012). *Property rights in personal data: A European perspective*. Kluwer Law International; Sold and distributed in North, Central, and South America by Aspen Publishers.
- Rouvroy, A., & Poullet, Y. (2009). The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy. In S. Gutwirth, Y. Poullet, P. De Hert, C. de Terwangne, & S. Nouwt (Eds.), *Reinventing Data Protection?* (pp. 45–76). Springer Netherlands. https://doi.org/10.1007/978-1-4020-9498-9_2
- Rule, J. B. (2012). “Needs” for surveillance and the movement to protect privacy. In *Routledge Handbook of Surveillance Studies*. Routledge. https://doi.org/10.4324/9780203814949.ch1_2_c
- Scott, J. W., & Keates, D. (Eds.). (2004). *Going public: Feminism and the shifting boundaries of the private sphere*. University of Illinois Press.

- Shephard, N. (2016). *Big Data and Sexual Surveillance* [APC Issue Papers]. Association for Progressive Communications. https://www.apc.org/sites/default/files/BigDataSexualSurveillance_0_0.pdf
- Sinders, C. (2020). *Feminist data set*. Clinic for Open Source Arts. <https://carolinesinders.com/wp-content/uploads/2020/05/Feminist-Data-Set-Final-Draft-2020-0517.pdf>
- Skinner-Thompson, S. (2020). *Privacy at the margins*. Cambridge University Press.
- Solove, D. J. (2002). Conceptualizing Privacy. *California Law Review*, 90(4), 1087–1155. <https://doi.org/10.2307/3481326>
- Squires, J. (2018). Public and private. In R. Bellamy & A. Mason (Eds.), *Political concepts*. Manchester University Press. <https://doi.org/10.7765/9781526137562.00015>
- Stachowitsch, S., & Sachseder, J. (2019). The gendered and racialized politics of risk analysis. The case of Frontex. *Critical Studies on Security*, 7(2), 107–123. <https://doi.org/10.1080/21624887.2019.1644050>
- Steinmüller, W., Lutterbeck, B., Mallmann, C., Harborth, U., Gerhard, K., & Schneider, J. (1971). *Grundfragen des Datenschutzes [Fundamental Questions of Data Protection]: Gutachten im Auftrag des Bundesministeriums des Innern [BT-Drs. VI/3816 Anlage 1]*. <https://dserver.bundestag.de/btd/06/038/0603826.pdf>
- Stolton, S. (2020, October 26). Poland rejects presidency conclusions on Artificial Intelligence, rights. *EURACTIV*. <https://www.euractiv.com/section/digital/news/poland-rejects-presidency-conclusions-on-artificial-intelligence-rights/>
- Suárez-Gonzalo, S. (2019). Personal data are political. A feminist view on privacy and big data. *Recerca.Revista de Pensament i Anàlisi*, 24(2), 173–192. <https://doi.org/10.6035/Recerca.2019.24.2.9>
- Supreme Court of India. (2017). *Justice K.S. Puttaswamy (Retd) ... Vs Union Of India* (D. Y. Chandrachud, Trans.). Union of India on. <https://indiankanoon.org/doc/91938676/>
- Taylor, L. (2017). Safety in numbers? Group privacy and Big Data analytics in the Developing World. In L. Taylor, F. Floridi, & B. Sloot (Eds.), *Group privacy – New challenges of data technologies* (pp. 13–36). Springer.
- Taylor, L., Floridi, L., & van der Sloot, B. (Eds.). (2017). *Group Privacy: New Challenges of Data Technologies*. Springer International Publishing. <https://doi.org/10.1007/978-3-319-46608-8>
- Theilen, J. T. (2021). *European Consensus between Strategy and Principle: The Uses of Vertically Comparative Legal Reasoning in Regional Human Rights Adjudication*. Nomos Verlagsgesellschaft mbH & Co. KG. <https://doi.org/10.5771/9783748925095>
- Tzanou, M. (2017). *The fundamental right to data protection: Normative value in the context of counter-terrorism surveillance*. Hart Publishing.
- Tzanou, M. (2020). The Future of EU Data Privacy Law: Towards a More Egalitarian Data Privacy. *Journal of International and Comparative Law*, 7(2), 449.
- Vergès, F. (2021). *A decolonial feminism* (A. J. Bohrer, Trans.). Pluto Press.
- Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, 4(5), 193–220. <https://doi.org/10.2307/1321160>
- Weinberg, L. (2017). Rethinking Privacy: A Feminist Approach to Privacy Rights after Snowden. *Westminster Papers in Culture and Communication*, 12(3), 5–20. <https://doi.org/10.16997/wpcc.258>

Whitman, J. (2003). The two Western cultures of privacy: Dignity versus liberty. *Yale Law Journal*, 113, 1151–1222. <https://doi.org/10.2307/4135723>

Wiener, A., Börzel, T. A., & Risse, T. (Eds.). (2018). *European integration theory* (Third edition). Oxford University Press.

Williams, P. J. (1995). *The alchemy of race and rights* (8. printing). Harvard Univ. Press.

Wischermann, U. (2003). Feministische Theorien zur Trennung von privat und öffentlich: Ein Blick zurück und auch nach vorn. *Feministische Studien*, 21(1), 23–34. <https://doi.org/10.1515/fs-2003-0104>

World Economic Forum. (2018). *The Global Gender Gap 2018* [Report]. World Economic Forum. <http://www.weforum.org/reports/the-global-gender-gap-report-2018>

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

Acknowledgments

Thank you to all reviewers for this special issue, whose work has enabled us to share these perspectives and to all participants of the Feminist Data Protection Workshop held in Berlin on 20 November 2019 for their input and discussions.

Published by



ALEXANDER VON HUMBOLDT
INSTITUTE FOR INTERNET
AND SOCIETY

in cooperation with



CREATE



centre
— internet —
et **societe**



R&I IN3
Internet
interdisciplinary
Institute
Universitat Oberta de Catalunya



UNIVERSITY OF TARTU
Johan Skytte Institute of
Political Studies