

Siapka, Anastasia; Biasin, Elisabetta

Article

Bleeding data: The case of fertility and menstruation tracking apps

Internet Policy Review

Provided in Cooperation with:

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

Suggested Citation: Siapka, Anastasia; Biasin, Elisabetta (2021) : Bleeding data: The case of fertility and menstruation tracking apps, Internet Policy Review, ISSN 2197-6775, Alexander von Humboldt Institute for Internet and Society, Berlin, Vol. 10, Iss. 4, pp. 1-34,
<https://doi.org/10.14763/2021.4.1599>

This Version is available at:

<https://hdl.handle.net/10419/250399>

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>



RESEARCH
ARTICLE



OPEN
ACCESS



PEER
REVIEWED

Bleeding data: the case of fertility and menstruation tracking apps

Anastasia Siapka *KU Leuven*

Elisabetta Biasin *KU Leuven*

DOI: <https://doi.org/10.14763/2021.4.1599>

Published: 7 December 2021

Received: 26 October 2020 Accepted: 12 April 2021

Funding: Anastasia Siapka's research is supported with a scholarship awarded by the Research Foundation - Flanders (FWO), Project No. 1151621N.

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: Siapka, A. & Biasin, E. (2021). Bleeding data: the case of fertility and menstruation tracking apps. *Internet Policy Review*, 10(4). <https://doi.org/10.14763/2021.4.1599>

Keywords: Data privacy, Fertility tracking, Consumer protection, Mobile apps

Abstract: Journalists, non-profits and consumer organisations, as well as the authors' first-hand review of relevant privacy policies reveal that fertility and menstruation tracking apps (FMTs) collect and share an excessive array of data. Through doctrinal legal research, we evaluate this data processing in light of data and consumer protection law but find the commonly invoked concepts of 'vulnerability', 'consent' and 'transparency' insufficient to alleviate power imbalances. Instead, drawing on a feminist understanding of work and the autonomist 'social factory', we argue that users perform unpaid, even gendered, consumer labour in the digital realm and explore the potential of a demand for wages.

This paper is part of **Feminist data protection**, a special issue of *Internet Policy Review* guest-edited by Jens T. Theilen, Andreas Baur, Felix Bieker, Regina Ammicht Quinn, Marit Hansen, and Gloria González Fuster.

Introduction

Tracking one's menstrual cycle is an ancient practice (Dean-Jones, 1989), which remained largely confined to the analogue world until the emergence of female technology (*femtech*) products and services. As the *femtech* market grew, fertility and menstruation tracking apps (hereafter FMTs) mushroomed in app stores and rose in popularity among adult and adolescent women (Moglia et al., 2016; Statista, 2020).¹ In terms of their main features, FMTs comprise a calendar overview of the menstrual cycle and a record of the user's symptoms, feelings, activities or analyses thereof. These are often complemented by health-related advice (e.g., blog posts, pop-up notifications, online courses) and communication channels (e.g., online forums, polls, chats).

Compared to jotting down the dates of their menses in a paper journal or calendar, the automation of menstruation tracking offers users a more comprehensive overview of the relevant information along with the ability to quickly analyse it. Such an analysis can, in turn, feed into decision-making around fertility treatment, contraception and conception (Gambier-Ross et al., 2018). Although both the accuracy and the efficacy of FMTs are contested (Moglia et al., 2016; Duane et al., 2016; Salleh & Taylor, 2019; Marsh, 2018), users report that such apps make it easier for them to observe (ir)regularities, inform gynaecologists or other physicians, anticipate their next period and accordingly manage work and holiday arrangements (Levy & Romo-Avilés, 2019). Moreover, FMTs often provide an online community, where users share experiences and concerns. This interaction, alongside the other app features, is valuable to users, who try to compensate for the lack of formal sexual and reproductive health education in what they perceive to be a safe environment (Gambier-Ross et al., 2018). Most importantly, users perceive this environment to be confidential and suitable for keeping 'their data private and inconspicuous' (Gambier-Ross et al., 2018). Hence, compared to regular offline or online calendars, which might be visible to others (e.g., their cohabitants or employers), users choose FMTs as a way to conceal menstruation and fertility

1. We acknowledge that not all users of FMTs are women. As not all those who menstruate identify as women and not all those who identify as women menstruate, we mainly refer to 'users' of FMTs or 'consumers', unless where being a woman is particularly relevant to our analysis.

(Karlsson, 2019).

Section 1: Data processing in FMTs

Notwithstanding the perceived advantages of FMTs, in interacting with them users voluntarily disclose intimate details about their menstrual cycle, sexual life and overall lifestyle; in addition, information such as device data or app usage data is automatically captured. By way of illustration, we identified the types of data the processing of which is explicitly mentioned in the privacy policies of six popular FMTs. Subsequently, these data were grouped into four main categories, which are listed below. A full breakdown of which types of data are processed by each FMT can be found in the Appendix to this article.²

- **Account data:**

Name/Username/Nickname, Email address, Gender, Date of birth, Password/pass-code, Location, ID number, Picture, Phone number, Time zone, Service preferences, Identifiers (e.g., profile ID, IP address, analytics IDs, conversation/consultation ID, messenger ID), Company, Purchasing/transaction data (e.g., shipping method, items ordered, discount, payment information, credit/debit card information), Language.

- **Health data:**

Body measurements, Body temperature, Menstrual cycle dates / period length, Various symptoms (e.g., pain, spotting, cravings, hair quality, productivity), Other information about health, wellbeing and activities (e.g., sexual activities), Health goals, Health-related information about child, Pregnancy-related information (e.g., day of conception, audio recordings, estimated due date).

- **Device data:**

Hardware model, Operating system, Unique device identifiers (e.g., IDFA), Mobile network information, Device storage information, Device settings, Application

2. Using the market research tool Apptopia, which specialises in app analytics, we searched for the most downloaded apps through Apple's App Store in the category Health & Fitness. The search was restricted to Belgium, in terms of its geographical scope, and to 24 April 2021, in terms of its temporal scope. From the resulting chart, we identified the top 3 free FMTs (i.e., Flo Pregnancy & Period Tracker [Flo], Clue Period, Ovulation Tracker [Clue] and Clover Period Tracker Calendar [Clover]) and the top 3 paid FMTs (i.e., Period Tracker Deluxe, Period Diary Pro and WomanLog Pro Calendar [WomanLog]). The sample was limited, as it only serves illustrative purposes. The types of data were sourced from the text of the privacy policies of these six in total apps (Flo, 2020; Clue, 2021; Wachanga, 2020; GP Apps, 2012; Bellabeat, n.d.; WomanLog, 2019). Where the different privacy policies of each app used different language to refer to the same types of data, we chose the broadest terms used.

identifier, Crash information, Browser, Browser settings, Manufacturer, Media Access Control address, Time-stamped logs of messages sent and received, Network status, Screen information, Mobile service provider, Installed app version, Applications installed in a mobile device.

- **App usage data:**

Frequency of use, General activity (e.g., visited areas/features, tabs opened, links/buttons clicked, sessions information, use patterns), Engagement with particular features/services, Acquisition channel / exit URLs, Authentication, Notification activity.

The list above indicates that fertility and menstruation tracking app users ‘bleed’ an excessive array of data, especially if we consider that the privacy policies of FMTs mention these types of data only as indicative, i.e., non-exhaustive examples. However, the extent of this data processing is unbeknown to many users (Gambier-Ross et al., 2018) and hard to comprehend, as empirical research on FMTs’ privacy policies has shown that information about data sharing remains obscure (Fowler et al., 2020). Most importantly, although users resort to FMTs in search of a private environment to log their menstruation dates, testing by journalists, non-profits and consumer organisations has demonstrated that FMTs shared users’ data with third parties, including Facebook (Privacy International, 2018, 2019; Schechner & Secada, 2019), Google (Quintin, 2017), entities involved in behavioural advertising and profiling (Forbrukerrådet, 2020), and research institutions (Palus, 2019). These revelations suggest that third-party sharing, especially for marketing and advertising purposes, is an integral part of FMTs’ business model rather than a one-off incident.

Nonetheless, compared to health and wellness applications in general (European Commission, 2014a, 2014b), legal research has paid little attention to the challenges of FMTs (e.g., Rosas, 2019) and even less to their particularly gendered dimensions. Our contribution attempts to bridge this gap by evaluating FMTs through the combined lens of feminism and law. In what follows, we assess the extent to which data protection and consumer protection law could tackle third-party sharing practices such as those mentioned above and we suggest a more radical approach based on feminist theory and political economy.

Section 2: The use of FMTs through the lens of data and consumer protection

The excessive data processing and third-party sharing in the context of FMTs illustrated in the previous section raises legal questions regarding data protection as well as consumer protection.³ Given that, as seen above, FMTs users are often unaware of how their data are (further) processed, the requirements chosen from both legislations were identified following a common theme, i.e., the means to counteract information and control asymmetries between FMTs users and providers. Hence, the following subsections investigate the notion of ‘vulnerability’ in privacy and consumer law, illustrate the requirements relevant to the mitigation of information imbalance, and present key limitations of these requirements.

FMTs through data protection laws

Imbalance of power and vulnerability: a data subject’s perspective

Where there is an imbalance of power, users’ autonomy may be at risk. For instance, FMTs users who are uninformed of the modalities of data processing will likely be unaware of the effects of their actions in the app’s environment. Or, not knowing who is further processing their personal data may lead users to lose control thereof. This eventuality becomes more evident if data concerning health or mood are used to profile users and nudge them into buying products when, according to the app’s predictive analysis, they might be more vulnerable.

Privacy and data protection legislation is a ‘manifestation of the idea that all individuals are vulnerable to the power imbalances created by data driven-technologies’ (Malgieri & Niklas, 2020, p. 2). The rationale for privacy protection is precisely addressing individuals’ vulnerability (Calo, 2018). Although the General Data Protection Regulation (GDPR or the Regulation) in its Recital 75 refers to vulnerable natural persons when assessing the risks to their rights and freedoms, it does not explicitly define the term ‘vulnerable data subject’. Nonetheless, Article 29 Data Protection Working Party ([WP29] 2017, p. 10) underlined that power imbalance is a crucial factor in identifying individual vulnerability. FMTs users may thus be seen as ‘vulnerable data subjects’. Power imbalance may occur when data subjects, here FMTs users, are unable to easily oppose the processing of their data or exer-

3. Due to space limitations, we address here a selection and brief overview of issues: vulnerability, consent and information asymmetry (see *infra*). Beyond data protection and consumer protection law, issues pertaining to content moderation and publishers’ liability would also be suitable for inclusion, given that some FMTs moderate, recommend and curate content produced by users and/or themselves. However, as such content moderation aspects are not central in FMTs, they are not examined in this article.

cise their rights. In any case in which an imbalance exists in the relationship between the data subject and the controller, also ‘in terms of possible impacts on fundamental rights and freedoms, significant information asymmetry based on predictive analytics’ (Malgieri & Niklas, 2020, p. 6), vulnerable data subjects can be identified (WP29, 2017).

Transparency and control, information and consent

Privacy and data protection laws furnish means useful for implementing fair, lawful and transparent personal data processing. The primary legal instrument for privacy and protection of personal data in the EU is the GDPR. The Regulation sets high standards for companies both inside and outside the EU, insofar as EU residents are being monitored. Following prior data protection laws, the GDPR maintains overarching principles to which data controllers must adhere, including transparency, purpose limitation, data minimisation, security and confidentiality, and storage limitation. Amongst others, GDPR tools that may strengthen users’ autonomy are information transparency, which should help FMTs users become aware of data processing, and the legal bases for processing, including consent, which should enhance users’ control over personal data.

Concerning information transparency, Articles 13 and 14 of the GDPR identify a list of elements that should be included when informing data subjects about the processing of their data. As Forbrukerrådet (2020) noted, the comprehensive data collection and sharing by such apps (often referred to as *adtech*) appears to be in conflict with the principle of transparency. Although promising, these requirements imply challenges in practice. For instance, controllers do not diligently map and record the third parties involved in the processing activity. On account of these challenges, subjects’ information rights are not always respected, for instance, the sub-processors of personal data are not disclosed, leaving subjects in obscurity with regard to third-party data outsourcing (Forbrukerrådet, 2020). Thus, notwithstanding the existing rules and guidance at national and EU level, it remains questionable whether such information criteria are rightfully operationalised in practice.

As regards the legal basis of FMTs’ data processing activities, some observations on the nature of personal data are needed. Menstruation data, users’ symptoms, moods, computation and evaluation thereof in the context of FMTs are ascribable to the GDPR’s ‘special categories of personal data’ (Article 9 GDPR), as they allow controllers to infer subjects’ health status (European Data Protection Supervisor [EDPS], 2015) or because they concern ‘a natural person’s sex life or sexual orien-

tation' (Article 9 GDPR). The processing of personal data and special categories thereof requires a legal basis, foreseen respectively in Articles 6 and 9 GDPR. For special categories of personal data notably, among the closed list of Article 9 GDPR, consent appears the most suitable legal basis for FMTs.

FMTs through the lens of consumer protection laws

Imbalance of power and vulnerability: a consumer's perspective

Imbalance of power and individual vulnerability is a consumer law concern, too. Over the last years, the advent of data-driven services online has fostered the relevance of consumer laws to digital content and services. In terms of consumer law, certain practices carried out by app providers, such as targeted advertisement to cause undue influence on users' behaviour, may have effects on consumers' autonomy and their ability to make decisions free from manipulation, especially when these practices occur without consumers' awareness. In this regard, parallel to the privacy and data protection requirements examined above, FMTs users may meet vulnerability profiles as consumers. The most relevant piece of EU legislation on consumer law is the Unfair Commercial Practice Directive (UCPD). This Directive was established in 2005 and amended in 2019 after the 'Consumers New Deal', which also introduced Directive 2019/770 on the supply of digital content and digital services. In contrast to the GDPR, the UCPD defines vulnerable consumers based on 'their mental or physical infirmity, age or credulity' (Article 5(3) UCPD). Such vulnerability might also be related to gender. A European Commission (2016a, p. 168) report explains that gender is a strong link with the dimension of consumer vulnerability. Other sources maintain that men are often less likely to be vulnerable than women on a number of indicators (Nardo et al., 2011, p. 12) and that pregnancy or significant life changes that women experience can be sources of vulnerability (The VOICE Group, 2010, p. 180).

Transparency and omission of information in misleading commercial practices

The UCPD prohibits commercial practices that are unfair, such as misleading or aggressive commercial practices (Articles 5-9 UCPD). Commercial practices are considered unfair when they materially distort or are likely to materially distort consumers' 'economic behaviour' (Article 5(2) UCPD). Examples of commercial practices that are considered *per se* unfair are provided in Annex I of the UCPD. A commercial practice is misleading if it contains false information, is untruthful, deceives or is likely to deceive the average consumer (Article 6 UCPD). A misleading practice could also occur through the omission of material information that consumers need in order to take an informed transactional decision that they would

otherwise not have taken (Article 7 UCPD). Transparency in data sharing is key in that regard. For example, providing an FMT without disclosing full information about the further sharing of personal data may constitute a misleading commercial practice. This is because, as the European Commission (2016b) observed, not informing the consumer that the data will be used for commercial purposes might constitute a misleading omission of material information, following Article 7(2) and No 22 of Annex I UCPD. In order not to be misled, consumers need to have, among other types, information on the extent of personal data processing necessary for service provision as well as information on any monetisation or third party sharing of the data (Helberger et al., 2017).

Evaluative remarks on data protection and consumer protection law

However appealing the notions of vulnerability, consent and transparency prevalent in data and consumer protection, they come with their own limitations, which are broached upon below.

The limitations of vulnerability: entrenching problematic assumptions

Emphasising vulnerability entails the risk of implying that there is a normative subject, that is, the average or reasonable data subject or consumer, from which the vulnerable individual deviates. Indeed, Recital 18 of the UCPD states that ‘this Directive takes as a benchmark the average consumer, who is reasonably well-informed and reasonably observant and circumspect’. Apart from the fact that such a binary seems too rigid, feminist philosophers of law have cast doubt on the concept of the ‘reasonable person’ as a reflection of male norms (Francis & Smith, 2021). Most importantly, by focusing on the deviation without challenging the norm, such an emphasis on vulnerability reinforces the status quo (Koivunen et al., 2018, pp. 2-5) and stigmatises the individual or group labelled as vulnerable (Fineman, 2010, p. 266). For feminist theorists, in particular, vulnerability ‘invoke[s] a problematic imaginary’ (Koivunen et al., 2018, p. 5), as it is associated with femininity, dependence, weakness, victimhood, deprivation and pathology (Fineman, 2010, p. 266; Koivunen et al., 2018, p. 5). As a result, the use of this concept can further consolidate static assumptions about lack of agency and uphold, among others, paternalistic and anti-feminist agendas (Koivunen et al., 2018, pp. 3-6).

Most importantly, vulnerability is a concept that accepts different interpretations. Article 5(3) of the UCPD adopts an understanding that ascribes vulnerability status to individuals or groups based on their characteristics rather than the situation(s) in which they find themselves. When vulnerability is thereby linked to consumers’

specific traits, the law can empower the individual so as to be more resilient. However, as long as the focus remains on specific individuals or groups and their labelling as vulnerable, the causes of possible harm, including structural injustices, remain intact and the social reasons or factors contributing to this vulnerability (such as market-related ones) remain unexplored. Hence, in line with Fineman, we should instead turn our attention to the unequal ways in which ‘systems of power and privilege [...] interact to produce webs of advantages and disadvantages’ (Fineman, 2008, p. 16).

The limitations of consent: how genuine is consent *vis-à-vis* power imbalance?

Although individuals appear concerned by the insufficient protection of their personal data, they tend to keep disclosing them in a seemingly careless way, giving rise to the so-called ‘privacy paradox’ (Barnes, 2006). Suárez-Gonzalo (2019, p. 176) attributes this paradox to power inequalities between individuals and those who exploit their data. At the same time, users are expected to resort to some sort of ‘privacy self-management’. While it appears as a promising solution—relying on individuals’ own capacity to evaluate the collection, use or disclosure of their information—privacy self-management is unlikely to be possible or feasible anymore (Solove, 2013) and could, among other practical problems, result in ‘consent fatigue’.

According to the GDPR, consent shall be freely given, specific, informed, explicit. ‘Freely given’ means that data subjects should have real choice and control: ‘[i]f the data subject has no real choice, feels compelled to consent or will endure negative consequences if they do not consent, the consent will not be valid’ (EDPB, 2020). However, when it comes to the role of consent as a means to balance control asymmetry, the GDPR’s conceptual framework is criticised as unable to protect users from data domination (Suárez-Gonzalo, 2019, p. 176). Suárez-Gonzalo (2019, p. 179) notes that consent cannot be guaranteed to always be specific and informed. Particularly in the case of FMTs examined in Section 1, specificity emerges as a challenge, given that their privacy policies mention the data processed only indicatively. More generally, the ‘freely given’ criterion is increasingly harder to meet if we consider users’ ongoing manipulation through behavioural advertising.

Furthermore, from a feminist orientation, consent serves as a ‘function of power’ (Marling, 2017). As Peña and Varon (2019, p. 27) note, ‘[r]ushly clicking a button to express accordance with all the conditions we listed above in a situation of power imbalance and practically no other option means we are currently deprived of no’. Conversely, through the lens of a feminist ethics of care, consent to privacy poli-

cies should be approached as an ongoing and mutually advantageous relationship between two equal parties rather than a box which needs to be ticked once by the user (Wittkower, 2016). In light of these concerns, ‘we should work towards new informed consent models in forms that consent can be genuine’ (Verhenneman, 2020, p. 305) or move beyond consent altogether.

The limitations of transparency: overlooking collective forms of data governance

Transparency requirements seem to assume that providing more information to users suffices to improve their position. However, as data processing and aggregation become more complex, ubiquitous and opaque, information asymmetries likewise grow (Ausloos, 2018, p. 14). Contrary to those data collectors who are equipped with data mining capabilities, even if app users are granted access to their own data, they remain deprived of the—computational but not only—power to process and meaningfully leverage these data; this recurrent state of powerlessness is described by Andrejevic (2014) as the ‘big data divide’. Even further, it is argued that the current data protection legal framework and transparency requirements fall short of ensuring effective answers to large parts of the social challenges implied in a machine learning big data context—especially when the data concern not only individuals but also groups (Vedder, 2018).

Indeed, scholars have criticised data protection for being too focused on the ‘individual’ level as a result of liberal privacy ideology (Suárez-Gonzalo, 2019). Second-wave feminism claimed that ‘personal is political’. According to Suárez-Gonzalo, it is necessary to reconsider the protection of personal data in light of such feminist claims which propounded overcoming the traditional opposition between the public and the private sphere. Therefore, if the ‘personal is political’, personal (data) should be considered as political and not confined into the realm of the household, private sphere. Instead, governing data should be seen as ‘a collective resource that necessitates far more democratic, as opposed to personal, forms of institutional governance’ (Viljoen, 2020, p. 9).

The limitations of law in general

Apart from the limitations of these specific concepts, appeals to data and consumer protection in general tend to privatise problems and do not lend themselves easily to collective considerations or negotiations. Above all, despite their differences, feminist theorists concur that power plays a role in what norms eventually become institutionalised and accepted as law, while conversely legal systems, aiming at the promotion of stability and order, legitimise the distribution of power in society (Francis & Smith, 2021). Indicatively, Lacey (1998; see also Jack-

son & Lacey, 2002) has consistently challenged the neutrality of state law and the public/private dichotomy, which is central to the privacy requirements examined in this article. As a result, power imbalances are hard to disrupt through the avenues of litigation or legislation (Anleu, 1992).

Overall, the challenges raised to the notions of vulnerability, consent and transparency as well as to law more broadly point to the need for structural and collective approaches in order to alleviate power imbalances.

Section 3: The use of FMTs through the lens of feminism and political economy

Although data protection and consumer protection law need not be rejected, a more structural and collective approach necessitates an investigation of more radical theories. As hinted in the challenges raised against vulnerability, consent and transparency, feminist theory highlights issues of subordination and power imbalance. Hence, this section relies on socialist feminism as a lens to evaluate the processing of FMT data.

Feminist perspectives to work and the ‘social factory’

The folk, as well as the legal, understanding of work focuses on the paid, contractual employment relationship that takes place in the public realm. Highlighting female-dominated activities, feminist theory and practice have challenged this restrictive understanding and the legitimacy of what is at each time perceived as work (Daniels, 1987). Against the traditional public/private demarcation, based on which the (remunerated) activity of male breadwinners occupies the public realm and the non-work activities of female spouses the private realm, feminists have argued that private and unpaid activity can likewise be work (Daniels, 1987). Even further, unpaid private activities are integral to the continuation and reproduction of paid ones (Dewart McEwen, 2018).

Despite the integral role that such private activities play for workers’ (re-)production as well as capital accumulation, the social system in which they take place avoids remunerating them by treating them as ‘a natural resource or a personal service’ outside capital (Federici, 2014, p. 8; see also Dalla Costa & James, 1975). Rather than arising naturally, Dalla Costa and James (1975) as well as Federici (2014) have argued that it was the advent of capitalism which caused the division between paid and unpaid labour and their respective association with factory work and housework. This division has further been gendered and hierarchical, with

women being relegated to a devalued domesticity (Davis, 1981). Nevertheless, an almost exclusive focus on the struggles of the male working class has overshadowed the unpaid female labour that takes place within the confines of the house (Fortunati, 1996). To counteract this omission, Dalla Costa and James (1975) call for the inclusion of housewives in our understanding of the working class. Hence, with women's domestic and, more relevant to this article, consumer labour being prominent examples of such unpaid private activities, feminism has long advocated for a reconceptualisation of work. Glazer (1984), indicatively, understands work as 'those activities which produce goods and/or provide services and/or provide for the circulation of goods and services which are directly or indirectly for capitalism', thereby questioning the rigid division between one's work being performed *for*, e.g., one's family or *for* capitalism (pp. 65-66).

Such a broad understanding of work is aligned with the autonomist concept of the social factory. The social factory refers to the phenomenon where 'various life processes, once deemed exterior to the commodity relation, have become integral to the economic calculations of capital' (Jarrett 2014, p. 140, as cited in Dewart McEwen, 2018, p. 238). It denotes the infiltration of work into new, hitherto unaffected, spaces and temporalities of the social fabric. One way in which the social factory extends its scope is by pulling consumers into the work process, namely assigning them tasks that paid employees were previously carrying out, albeit without acknowledging them as parts of the wage relationship. Likewise, feminist theory draws attention to the ways in which this re-organisation of work affects mostly female consumers, for example with the introduction of self-service checkout in retail stores (Glazer, 1984). Bringing this shift to the digital media context, Terranova (2000) links the concept of the social factory to the digital economy, and construes creating and editing websites or software, participating in mailing lists and chats, or sharing stories online as free, meaning unpaid, labour. Adding a gendered dimension to this view, Jarrett (2016) introduces the notion of the 'digital housewife', likening the unpaid consumer labour that takes place online to the unpaid houseworkers' labour in the domestic sphere: '[l]ike housewives, consumers receive little or no direct financial compensation for their contribution to the revenue-generating mechanisms of digital media sites so that all of their labour produces surplus value for the website provider' (p. 11).

Data sharing in FMTs as free, digital labour

As indicated in the introduction, users might be experiencing their interaction with FMTs as useful to their self-knowledge and self-improvement. Nonetheless, in line with the above mentioned feminist view of work and the concept of the social fac-

tory, we contend that they equally produce value for capital in multiple, ongoing ways. Dewart McEwen (2018) has argued that self-tracking practices constitute digital labour when (i) they beget data-as-commodity and feed digital networks with content; (ii) reproduce labour; and (iii) nurture subjectivities which match the consumption and production needs of the social factory. FMTs meet all these conditions.

First and foremost, FMTs are grounded in the commodification of users' data. By inserting detailed information about their physiological, behavioural or emotional state, users generate data which, both on their own and as prime material for analysis, are of 'commercial, managerial and research value' (Lupton, 2015a). As this value is mainly attributed to data about biological material (i.e., menstrual blood) and bodily functions, it can further be considered a type of 'biovalue', similarly to body parts, cells and tissues (Lupton, 2016). This value is manifest in marketers' perception of people who are trying to conceive or have already conceived as a highly marketable demographic, especially for retail purposes (Duhigg, 2012; Tiffany, 2018; Weigel, 2016), and in their concomitant willingness to pay more for the latter's data than that of other users (Lupton, 2015a). Similarly, information about women's hormonal cycles provides insights to their expected consumer behaviour that are useful to marketers (Durante et al., 2011). Hence, users' data entries are leveraged for marketing campaigns, targeting both potential and existing users. In this way, they substitute for the work that market researchers would otherwise carry out themselves.

It follows that users' data are valued not only for their utility in the context of menstruation tracking *per se* (use-value) but also for their relative value as insights useful to marketing or other purposes and external actors (exchange-value). As such, they undergo a process of commodification, whereby the latter implies the transformation of use-values into exchange-values (Mosco, 2009). Three features of FMTs mainly aid this commodification. At a first stage, gamification invites users to stay engaged with the app and insert data, especially the types of data that are most fruitful in the digital economy (Dewart McEwen, 2018). Playful elements make the time spent in the app's environment resemble games rather than work. Subsequently, more time spent in the app equals more user data harvested and potentially sold as well as more exposure to advertisements, converting usage time to productive labour time (Fuchs, 2014). Next, FMTs are an exemplary manifestation of the 'quantified self' movement. Quantification converts the embodied knowledge of one's messy, unruly or shameful corporeal experience to disembodied, sterilised, mathematically commensurable and thereby amenable to commodi-

fication data pieces or packages. Lastly, algorithmic processing captures and transforms said data. Users cannot, by their own means, extract the value inherent in their data; rather, there is a gap between them and the algorithmic expertise enclosed in the providing company (Dewart McEwen, 2018). The same applies to data brokers and marketing companies with the expertise to link existing, disparate data points, find correlations and patterns among them, and turn them into new outputs.

In addition, feminism has drawn attention to the female work of community-making, which, despite preserving society, is relegated to a voluntary activity (Daniels, 1987). As a descendant of care-giving and household management, community-making has long been viewed as an altruistic provision by women, not a commercial service. This view encompasses offline as well as online communities. In reference to consumer labour in digital media, Jarrett (2014) mentions managing community forums and commenting on social media as examples of practices that engender 'social cohesion or dependency as well as [...] the intellectual and creative commons shared by all users' (p. 19). Indeed, users produce value by contributing content that sustains FMTs' functions and knowledge exchange. As user-generated content is encouraged and shared through forums and chats, users eventually feed digital networks with content and thereby facilitate the creation of community as commodity.

Second, as users report, FMTs help them anticipate emotional or bodily changes and accordingly schedule work obligations (Levy & Romo-Avilés, 2019) or avoid negative evaluations by colleagues (Karlsson, 2019). Broadly put, the management of one's menstruation is conducive to better, more reliable execution of one's work responsibilities. FMTs providers even advocate for menstruation management as a productivity tool, especially for specific professions (Fabiano, 2019; Mysoor, 2018; Saner, 2019). In facilitating their capacity to work, the activities of FMTs users could be considered a form of reproductive labour, meaning 'the socially necessary and often unpaid work of caring for and reproducing the labourer's body and mind' (Dewart McEwen, 2018, p. 244). FMTs assist the allocation of human and non-human resources at a broader, workplace level, too: there are already employers who actively encourage personnel to track and share data with them through FMTs with the aim of decreasing healthcare coverage and ensuring that women do not lose productivity hours in fertility treatments (Harwell, 2019).

Finally, the cultivation of market-aligned subjectivities, which will be conducive to production and consumption, as well as the cultivation of norms and identities that subjects will adopt and reproduce (Charitsis, 2018) facilitates the creation of

further value for FMTs and digital capitalism in general. For Lupton (2015b), the constant record-keeping and self-management solicited by FMTs normalises ‘an algorithmic subjectivity, in which the body and its health states, functions and activities are portrayed and understood predominantly via quantified calculations, predictions and comparisons’ (p. 449). Thereby stimulating the desire to optimise and quantify knowledge about one’s self through digital means, FMTs shape self-regulating subjects who are more likely to share valuable information and content with them. Hence, the data that users generate to improve their well-being ultimately backfire: such data serve to further manipulate the same users’ needs, desires and behaviour for the sake of advancing commercial interests. For Andrejevic (2013), ‘[t]o the extent that consumers participate in generating the information that feeds into the manipulation process, we might level the charge of exploitation to highlight the way in which the capture of personal information turns our own activity against ourselves’ (p. 158).

Based on the above, by sharing their data, users create and augment the value of such apps, together with that of component or affiliated products and services, in ways that often exceed their awareness or control. The fruits of their activity become resources that benefit the companies processing these data alongside the latter’s business partners—Glow, for example, partners with pharmacies and fertility clinics (Hall, 2017). As FMTs users become active participants in the production process, the demarcation between who produces, consumes and benefits from their data fades: they become ‘prosumers’ (Toffler, 1980), standing in-between value consumption and production (Charitsis, 2016; Lupton, 2015b). Such prosumption becomes clearer when conceived not only in terms of each user’s contribution, but also in terms of the collective value created through their totality. More broadly, even when the value produced is not extracted by the app providers and partners directly, it indirectly reproduces (digital) capitalism, meeting Glazer’s broad definition of work from the previous sub-section. Therefore, using an FMT might concurrently be a leisurely, handy or meaningful activity and, insofar as it is not adequately rewarded, an exploited one.

This unwaged labour can further be interpreted as gendered (Dewart McEwen, 2018). Like the male breadwinners benefitting from their spouses’ unpaid domestic labour, the industry capitalising on FMT data and users’ invisible labour is male-dominated, with some of the most popular FMTs (i.e., Flo, Glow and Ovia) having male Chief Executive Officers, while another one, Femm, was funded by ‘anti-abortion, anti-gay Catholic campaigners’ (Glenza, 2019). Albeit beyond this paper’s limitations, it is worth exploring the implications of this composition for pa-

triarchal relations, power imbalances and the gendered division of labour. Furthermore, as alluded above, the results of such labour might be used for categorising and targeting of, among others, FMTs users themselves with—mostly pregnancy-related—ads, leading to their gendered exploitation.

The digital nature of this labour is likewise pertinent. Ekbja and Nardi have explored what could be a tendency contrary to automation: they define ‘heteromation’ as ‘the extraction of economic value from low-cost or free labor in computer-mediated networks’ (Ekbja & Nardi, 2017, p. 1). Crucially, in the context of heteromation, FMTs users lack autonomy, so they are confined to a state of heteronomy and, albeit unpaid, their work replaces that of paid employees (e.g., market researchers) and increases corporate profits (Ekbja & Nardi, 2017).

Wages for FMT data?

Could the answer to this generation of value by users be their compensation? Again, feminist struggles regarding domestic labour, particularly the demand for wages against housework, as articulated in the eponymous manifesto (Federici, 1975), could prove an alternative reaction to ‘heteromation’. Indeed, the ‘wages for Facebook’ and ‘Pay Me Facebook’ initiatives (Jung, 2014; Ptak, 2014) demonstrate how a demand originating in Italy of the 1970s could apply to today’s worldwide digital labour.

The potential of the demand for wages

We identify three main advantages in such a demand. In a first instance, visibility lends legitimacy to one’s work and is a precondition for successfully resisting or struggling against that work (Federici, 1975). In the same vein as ‘wages against housework’ and ‘wages for Facebook’, requesting wages for the data that FMT users share could, therefore, stimulate critical debate. It could garner social and institutional recognition for users’ contribution and its quantifiable value as well as capturing users’ distinct status as ‘prosumers’ beyond the data subject/controller or consumer/producer binaries. In addition, as Federici (2012) has noted, ‘[i]t seems to be a social law that the value of labor is proven and perhaps created by its refusal. This was certainly the case of housework which remained invisible and unvalued until a movement of women emerged who refused to accept reproduction work as their natural destiny.’ (p. 96). Similarly, demanding wages for FMT data could empower the apps’ users to refuse this type of unpaid consumer labour. Most importantly, and in contrast to the legal requirements previously examined, such empowerment would not rely on users’ problematic characterisation as vulnerable.

In a second instance, demands for wages come with a provisional recognition of those demanding as workers. As such, they would enhance users' bargaining power and enable them to negotiate the terms and extent of their contribution to such apps, a possibility which is currently precluded by the 'take it or leave it' nature of consent requirements. Moreover, compared to the individualistic nature of data protection and consumer protection laws in general, such a demand would offer the opportunity for collective bargaining and negotiations. It would be a direct demand for power premised upon the shared experience of data production and processing and the equally shared need for better conditions if one is to keep engaging in such production.

Lastly, 'to demand wages for housework is to make it visible that our minds, bodies and emotions have all been distorted for a specific function, in a specific function, and then have been thrown back at us as a model to which we should all conform if we want to be accepted as women in this society' (Federici, 1975, p. 5). Requesting that an activity be recognised as work and therefore compensated serves to recognise that this activity comes with its own standards of mental, physical and emotional excellence. Depending on individuals' adherence to these standards, some will be positioned as good or superior and others as bad or inferior. Similarly, FMTs construct and reinforce norms that 'order and stratify menstruation and menstruating', aptly summarised as 'menstrunormativity' (Persdotter, 2020). Users, in turn, might internalise these norms and position themselves as normal or healthy versus abnormal or unhealthy menstruators. Demanding wages for FMT data would be an alternative way to illuminate users' engagement and even struggle with such norms.

The limitations of the demand for wages

However, such a recognition is not without concerns. First, accepting wages in exchange for data might be received as a sort of ratification of this unpaid user-driven labour, which can backtrack rather than accelerate users' empowerment. If we accept that this relation enters the realm of employment, then the power asymmetries and hierarchies of the workplace might be reproduced. One might wonder, for example, if we recognise data provision as work does it follow that users should comply with directions from those for whom they work, i.e., the data controllers? Such an outcome seems off-putting.

Second and related, linking data collection with wages might enhance the same logic of accumulation that the feminist, autonomist thinking seeks to criticise. The existence of compensation is likely to act as an incentive for users to give more of

their privacy away. This, in turn, could support even more the formation of market-aligned subjectivities and change users' perspective on themselves.

However, none of these two objections constitutes a fatal blow to the demand for wages. Specifically, if the remuneration of users did not take the form of a wage conditional on the extent of users' contribution but that of an unconditional and fixed Universal Basic Income, which would be funded by the redistribution of the profits generated by those data, it would not be necessary to affirm a working relationship between FMTs users and providers. Also, as the amount received would be fixed, users would not have any particular incentive to share more rather than less data.

Third, demanding wages for data might imply that the data we generate are a piece of property which can be alienated from ourselves, measured, reused and sold in the market. However, it is crucial not to forget that these data are often about female bodies, which feminist thought has recognised as 'the main targets, the privileged sites, for the deployment of power techniques and power-relations' (Federici, 2014, p. 15). Encouraging the commodification of such embodied data and subjecting them to market norms would, therefore, oppose this line of thinking.

As with the previous ones, though, this objection is not absolute. Given that anti-commodification arguments tend to be more strongly raised in relation to women rather than men, possibly owing to a romantic essentialism of the former (Silbaugh, 1997), it should be approached from a critical and balanced perspective. Such a perspective could be critical in the sense of acknowledging that a refusal of this monetary framework of data sharing in the interest of anti-commodification might actually reinforce the idea that women and their activities lie outside the market realm and might thereby bear economically disempowering implications for women and FMTs users in general. It could further be balanced by recognising that such a monetary framework does not have to exclude other, non-market ways of conceiving users' bodies and the data derived from those; rather, multiple ways of understanding and valuing users' activities, bodies and data could co-exist.

Fourth, and most important, a demand for wages could be characterised as unrealistic or too distant from the current legal landscape. Federici (1975) herself describes such calls as 'demanding the impossible', considering that their practical applicability is dubious. Indeed, evidence in that direction comes from repeated US case law. In the illustrative case of *Hallissey et al v. America Online, Inc*, volunteers of AOL's Community Leader programme asked to be considered employees and be

granted wages for their work as moderators (Kirchner, 2011). Although AOL eventually settled with the plaintiffs, the court did not bring the case to trial (Kirchner, 2011). In *Jeung v. Yelp, Inc.* the court denied Yelp reviewers the status of employees, and rejected their compensation claims (Goldman, 2015). Similarly, in *Rojas-Lozano v. Google Inc.*, the plaintiff argued that the second of the two letter sequences she had to decipher when signing up for an email account was not necessary for security purposes; rather, it was improving Google's digitisation service which the company offered for profit to third parties (Dinzeo, 2016). However, the court did not uphold the plaintiff's claim that Google was unfairly benefitting from her labour, and maintained that the benefit of accessing free email services was overriding (Dinzeo, 2016). Although these cases are mostly relevant to the US context, they are telling of courts' reluctance to accept compensation requests by platform or website contributors. Even where plaintiffs' value contributions were recognised, they were still considered as falling outside the employment relationship.

Nevertheless, evidence towards the opposite direction comes from the EU itself and particularly from the debate preceding the adoption of Directive 2019/770 on the provision of digital content and services. Directive 2019/770 recognised that personal data, although they should not be considered a tradeable commodity (Recital 24), can be provided by the consumer to the trader for the purpose of supplying a digital service (Article 3 Directive 2019/770, see also Helberger et al., 2017, p. 27). The Directive's original proposal referred to the consumer as actively providing 'counter-performance other than money in the form of personal data or any other data' (European Commission, 2015).⁴ The scrutiny of Directive 2019/770 opened ways to further conceptualise the provision of personal data as part of a mutual contractual relationship with the provider of a digital service. How should we characterise the relationship between consumers (and thus FMTs users) and the digital service providers to which the former provide their personal data? Will 'data monetisation' be possible?

The first question is far from settled in legal doctrine. Traditionally, some maintain that privacy, as a fundamental right, is undeniable and unavailable for commercialisation ('moral approach'). Others consider data as susceptible to contractual negotiations, given that they incorporate economic value and correspond to a patrimonial interest of the subjects involved ('contractual approach') (D'Ippolito, 2020).

4. However, the actual formulation differs, as the EDPS (2017) was concerned that said proposal would alter the fundamental rights' balance struck in the GDPR. Consequently, the EDPS advised against it.

Some even hypothesise that users should be remunerated by the controller, further to the use of data relating to them (*idem*). Resta and Zeno-Zencovich (2018) offer such a ‘reversing’ perspective, observing that ‘it is users that provide a service (the data) to certain businesses, which are in turn remunerated with digital services’ (p. 417).⁵ Regarding the second question, some maintain it could be possible to estimate the value of personal data (Malgieri & Custers, 2018, p. 289) to the point that there should exist a ‘right to know the value of personal data’ (*idem*; Malgieri & Custers, p. 303; contrariwise EDPS, p. 10). These two crucial questions are underpinned by a broader enquiry about the nature of personal data. Currently, scholars are intensely debating on the notions of data ownership and property, or other, rights over data (see e.g., Zech, 2017; Stepanov, 2020; Hugenholtz, 2018). These questions remain open but their resolution could determine the nature of the relationship between FMTs users and providers.

Overall, the above-mentioned (yet rejected) proposal of the Directive appears consistent with the feminist thought on unpaid labour examined above, since it provides an interesting avenue for hypothesising economic wages to acknowledge and compensate the generation of value by FMTs users. Nonetheless, the concerns raised thus far indicate that the mere distribution of monetary rewards would not necessarily serve as a panacea for eradicating all power asymmetries in the context of data sharing. Hence, further research is needed regarding the nature of such a contractual relationship and of the data generated as well as regarding the more practical and systemic ways in which rewards for users’ data could be introduced.

Conclusion

Notwithstanding their perceived benefits, FMTs gather an extensive array of user data, which their providers reportedly share with third parties for, among others, commercial purposes. This issue falls directly within the scope of data protection and consumer protection legislation. Nonetheless, as selectively illustrated, the concepts of vulnerability, transparency and consent which dominate in the relevant legal discourse are inadequate to alleviate the power imbalances observed in the context of FMTs and do not sufficiently address the challenges faced by FMTs users. Rather, the latter’s position in the legal landscape appears tainted by legal uncertainty. The law recognises such users as data subjects and consumers; yet,

5. Provocatively, the former president of the Italian data protection Supervisory Authority noted ‘[a] new digital underclass is emerging, a “Fifth Estate” made up of those who are willing to give up their freedom with their data, in exchange for services offered online only apparently “at zero price”’ (Soro, 2019, p. 7).

one may wonder if there is room to legally classify them as prosumers. In this direction, Marsden (2018) advocates for a new type of ‘prosumer law’ that ‘draws on competition, technology regulation, fundamental human rights, privacy, and free expression’ (pp. 378-379). It might be too early or unrealistic to give definite answers to this question. However, evaluating the contractual nature of the provision of personal data as a service could be an interpretative way forward.

Such an interpretation would also be more aligned with feminist thinking. Drawing on a feminist theory and political economy perspective, and particularly on the broad understanding of work inherent in feminism alongside the autonomist concept of the social factory, we assessed the value generated by FMTs users and appropriated by the apps’ providers. Specifically, in sharing their data with FMTs, users produce value that benefits FMTs providers, their partners, and (digital) capitalism more broadly. This value manifests itself in the form of commodification of user data, online community-making, reproductive labour, and the cultivation of market-aligned, algorithmic subjectivities, leading to its characterisation as unpaid, digital and, to a certain degree, gendered consumer labour. As a next step, in accordance with the adopted perspective, the recognition of such labour should take the form of a demand for wages. Yet, such a demand is not meant to be taken literally and has its own limitations, which merit analysis. All things considered, though, it constitutes a demand of high heuristic potential, allowing us to fathom and expose the economic relations sustaining FMTs. It is the functional equivalent of a refusal to perform unpaid consumer labour, an expression of collective solidarity, a way to politicise this condition of exploitation and unsettle what we have come to accept as normal and, consequently, a stimulus for much needed legal reform that would capture these problematic economic relations more accurately.

Finally, while keeping in mind that data should not be viewed solely as a commodity, new perspectives opened by the Directive 2019/770 and by the, even theoretical, discussion of data provision in exchange for services might prove useful in more accurately reflecting the realities of the value-producing relations in FMTs and similar apps. Such a potentially synallagmatic approach could provide new theoretical and practical scaffolding to, on the one hand, recognise the value that users’ ‘bleeding’ data yield, and, on the other, curtail the ‘leaky’ processing activities that app providers deploy.

References

1. Andrejevic, M. (2013). Estranged Free Labor. In T. Scholz (Ed.), *Digital Labor: The Internet as Playground and Factory* (pp. 149-164). Routledge. doi: <https://doi.org/10.4324/9780203145791>
2. Andrejevic, M. (2014). Big Data, Big Questions| The Big Data Divide. *International Journal of Communication*, 8, 17. ISSN 1932-8036
3. Article 29 Data Protection Working Party. (2017). *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679* (WP 248 rev.01; p. 22). http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236
4. Barnes, Susan B. (2006). A privacy paradox: Social networking in the United States. *First Monday*, 11(9), 1-10. doi: <https://doi.org/10.5210/fm.v11i9.1394>
5. Bellabeat. (n.d.). *Privacy policy*. Bellabeat. Retrieved 25 April 2021, from <https://bellabeat.com/privacy-policy/>
6. Calo, R. (2018). Privacy, Vulnerability, and Affordance. In E. Selinger, J. Polonetsky, & O. Tene (Eds.), *The Cambridge Handbook of Consumer Privacy* (pp. 198–206). Cambridge University Press. doi: <https://doi.org/10.1017/9781316831960.011>
7. Charitsis, V. (2016). Prosuming (the) self. *Ephemera : Theory and Politics in Organization*, 16(3), 37–59. ISSN 1473-2866
8. Charitsis, V. (2018). *Self-tracking, datafication and the biopolitical prosumption of life*. <http://urn.kb.se/resolve?urn=urn:nbn:se:kau:diva-66177>. ISBN: 978-91-7063-934-0
9. Clue. (2021, February 23). *Privacy Policy*. Clue. <https://helloclue.com/privacy>
10. Dalla Costa, M., & James, S. (1975). *The power of women and subversion of the community* (3rd ed.). Falling wall press. ISBN: 978-0-9502702-4-1
11. Daniels, A. K. (1987). Invisible Work 1987 SSSP Presidential Address. *Social Problems*, 34(5), 403–415. doi: <https://doi.org/10.2307/800538>
12. Davis, A. Y. (1981). The Approaching Obsolescence of Housework: A Working-Class Perspective. In *Women, race, & class* (1st ed). Random House.
13. Dean-Jones, L. (1989). Menstrual Bleeding according to the Hippocratics and Aristotle. *Transactions of the American Philological Association* (1974-), 119, 177. doi: <https://doi.org/10.2307/284268>
14. Dewart McEwen, K. (2018). Self-Tracking Practices and Digital (Re)productive Labour. *Philosophy & Technology*, 31(2), 235–251. doi: <https://doi.org/10.1007/s13347-017-0282-2>
15. Dinzeo, M. (2016, February 5). *Google Ducks Gmail Captcha Class Action*. Courthouse News Service. <https://www.courthousenews.com/google-ducks-gmail-captcha-class-action/>

16. D'Ippolito, G. (2020). Commercializzazione dei dati personali: il dato personale tra approccio morale e negoziale. *Il Diritto dell'Informazione e dell'Informatica*, XXXV(4), 635–675. <http://hdl.handle.net/11590/387597>
17. Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive'), European Parliament, Council of the European Union, OJ L 149 (2005). <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:32005L0029>
18. Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services, PE/26/2019/REV/1, European Parliament, Council of the European Union, OJ L 136 (2019).
19. Duane, M., Contreras, A., Jensen, E. T., & White, A. (2016). The Performance of Fertility Awareness-based Method Apps Marketed to Avoid Pregnancy. *The Journal of the American Board of Family Medicine*, 29(4), 508–511. doi: <https://doi.org/10.3122/jabfm.2016.04.160022>
20. Duhigg, C. (2012, February 16). How Companies Learn Your Secrets. *The New York Times*. <https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html>
21. Durante, K. M., Griskevicius, V., Hill, S. E., Perilloux, C., & Li, N. P. (2011). Ovulation, Female Competition, and Product Choice: Hormonal Influences on Consumer Behavior. *Journal of Consumer Research*, 37(6), 921–934. doi: <https://doi.org/10.1086/656575>
22. Ekbia, H. R., & Nardi, B. A. (2017). *Heteromation, and Other Stories of Computing and Capitalism*. The MIT Press. <https://mitpress.mit.edu/books/heteromation-and-other-stories-computing-and-capitalism>. ISBN: 9780262036252
23. European Commission. (2014a). *COMMISSION STAFF WORKING DOCUMENT on the existing EU legal framework applicable to lifestyle and wellbeing apps* (Accompanying the Document GREEN PAPER on Mobile Health ('mHealth') SWD(2014) 135 final). https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=5146
24. European Commission. (2014b). *GREEN PAPER on mobile Health ('mHealth')* (COM(2014) 219 final). <https://ec.europa.eu/transparency/regdoc/rep/1/2014/EN/1-2014-219-EN-F1-1.Pdf>
25. European Commission. (2015). *Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on certain aspects concerning contracts for the supply of digital content* (COM/2015/0634 final-2015/0287 (COD)). European Commission. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015PC0634>
26. European Commission. (2016a). *Consumer vulnerability across key markets in the European Union—Final report*. European Commission.

- https://ec.europa.eu/info/sites/info/files/consumers-approved-report_en.pdf
27. European Commission. (2016b). *COMMISSION STAFF WORKING DOCUMENT GUIDANCE ON THE IMPLEMENTATION/APPLICATION OF DIRECTIVE 2005/29/EC ON UNFAIR COMMERCIAL PRACTICES Accompanying the document COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS A comprehensive approach to stimulating cross-border e-Commerce for Europe's citizens and businesses* (SWD/2016/0163 final). European Commission. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016SC0163>
 28. European Data Protection Board. (2020). *Guidelines 05/2020 on consent under Regulation 2016/679* [Guidelines]. European Data Protection Board. https://edpb.europa.eu/sites/edpb/files/file1/edpb_guidelines_202005_consent_en.pdf
 29. European Data Protection Supervisor. (2015). *Mobile Health—Reconciling technological innovation with data protection* (Opinion 1/2015). European Data Protection Supervisor. https://edps.europa.eu/sites/edp/files/publication/15-05-21_mhealth_en_0.pdf
 30. European Data Protection Supervisor. (2017). *Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content* [Opinion]. European Data Protection Supervisor. https://edps.europa.eu/sites/edp/files/publication/17-03-14_opinion_digital_content_en.pdf
 31. Fabiano, J. (2019, June 25). *How women can use their menstrual cycles to optimize their work schedules*. LADDERS. <https://www.theladders.com/career-advice/menstrual-cycle-optimize-work-schedule>
 32. Federici, S. (1975). *Wages Against Housework*. Power of Women Collective and Falling Wall Press. <https://caringlabor.files.wordpress.com/2010/11/federici-wages-against-housework.pdf>
 33. Federici, S. (2012). The Reproduction of Labor Power in the Global Economy and the Unfinished Feminist Revolution (2008). In *Revolution at Point Zero: Housework, Reproduction, and Feminist Struggle* (pp. 91–114). PM Press. ISBN: 978-1-60486-333-8
 34. Federici, S. (2014). *Caliban and the witch* (2., rev. ed). Autonomedia. ISBN: 978-1-57027-059-8
 35. Fineman, M. (2008). The Vulnerable Subject: Anchoring Equality in the Human Condition. *Yale Journal of Law & Feminism*, 20(1). <https://digitalcommons.law.yale.edu/yjlf/vol20/iss1/2>
 36. Fineman, M. (2010). The Vulnerable Subject and the Responsive State. *Emory Law Journal*, 60(2), 251. ISSN: 0094-4076
 37. Flo. (2020, August 7). *Flo Privacy Policy*. Flo. <https://flo.health/privacy-policy>
 38. Forbrukerrådet. (2020). *OUT OF CONTROL: How consumers are exploited by the online advertising industry*. <https://fil.forbrukerradet.no/wp-content/>

- uploads/2020/01/2020-01-14-out-of-control-final-version.pdf
39. Fortunati, L. (1996). *The arcane of reproduction: Housework, prostitution, labor and capital* (J. Fleming, Ed.; H. Creek, Trans.). Autonomedia. ISBN: 978-0-936756-14-1
 40. Fowler, L. R., Gillard, C., & Morain, S. R. (2020). Readability and Accessibility of Terms of Service and Privacy Policies for Menstruation-Tracking Smartphone Applications: *Health Promotion Practice*. doi: <https://doi.org/10.1177/1524839919899924>
 41. Francis, L., & Smith, P. (2021). Feminist Philosophy of Law. In E. N. Zalta (Ed.), *The Stanford Encyclopedia of Philosophy* (Spring 2021). Metaphysics Research Lab, Stanford University. <https://plato.stanford.edu/archives/spr2021/entries/feminism-law/>
 42. Fuchs, C. (2014). Digital prosumption labour on social media in the context of the capitalist regime of time. *Time & Society*, 23(1), 97–123. doi: <https://doi.org/10.1177/0961463X13502117>
 43. Gambier-Ross, K., McLernon, D. J., & Morgan, H. M. (2018). A mixed methods exploratory study of women's relationships with and uses of fertility tracking apps. *DIGITAL HEALTH*, 4, 2055207618785077. doi: <https://doi.org/10.1177/2055207618785077>
 44. Glazer, N. Y. (1984). Servants to Capital: Unpaid Domestic Labor and Paid Work. *Review of Radical Political Economics*, 16(1), 60–87. doi: <https://doi.org/10.1177/048661348401600106>
 45. Glenza, J. (2019, May 30). Revealed: Women's fertility app is funded by anti-abortion campaigners. *The Guardian*. <http://www.theguardian.com/world/2019/may/30/revealed-womens-fertility-app-is-funded-by-anti-abortion-campaigners>
 46. Goldman, E. (2015, August 17). *Court Says Yelp Reviewers Aren't Employees*. Forbes. <https://www.forbes.com/sites/ericgoldman/2015/08/17/court-says-yelp-reviewers-arent-employees/>
 47. GP Apps. (2012, June 18). *Privacy Policy*. GP Apps. <https://gpapps.com/support/privacy-policy/>
 48. Hall, M. (2017, July 25). *The Strange Sexism of Period Apps*. VICE. <https://www.vice.com/en/article/qvp5yd/the-strange-sexism-of-period-apps>
 49. Harwell, D. (2019, April 10). *Tracking your pregnancy on an app may be more public than you think*. The Washington Post. https://search-proquest-com.kuleuven.ezproxy.kuleuven.be/docview/2205929632?rfr_id=info%3Axri%2Fsid%3Aprimio
 50. Helberger, N., Borgesius, F. Z., & Reyna, A. (2017). The perfect match? a closer look at the relationship between EU consumer law and data protection law. *Common Market Law Review*, 54(5), 1427–1465. ISSN: 0165-0750
 51. Hugenholtz, P. B. (2018). Against 'Data Property'. In H. Ullrich, P. Drahos, & G. Ghidini (Eds.), *Kritika: Essays on Intellectual Property* (Vol. 3, pp. 48-71). (Kritika; Vol. 3). Cheltenham: Edward Elgar. doi: <https://doi.org/10.4337/>

9781788971164.00010

52. Jackson, E., & Lacey, N. (2002). Introducing feminist legal theory. In J. E. Penner, D. Schiff, R. Nobles, & A. Barron (Eds.), *Introduction to jurisprudence and legal theory: Commentary and materials* (pp. 779–853). LexisNexis Butterworths. ISBN: 978-0-406-94678-2
53. Jarrett, K. (2014). The Relevance of “Women’s Work”: Social Reproduction and Immaterial Labor in Digital Media. *Television & New Media*, 15(1), 14–29. doi: <https://doi.org/10.1177/1527476413487607>
54. Jarrett, K. (2016). *Feminism, Labour and Digital Media: The Digital Housewife*. Routledge. ISBN: 978-1-315-72011-1
55. Jung, E. A. (2014). Wages for Facebook. *Dissent Magazine*. <https://www.dissentmagazine.org/article/wages-for-facebook>
56. Karlsson, A. (2019). A Room of One’s Own? *Nordicom Review*, 40(s1), 111–123. doi: <https://doi.org/10.2478/nor-2019-0017>
57. Kirchner, L. (2011, February 10). *AOL Settled with Unpaid “Volunteers” for \$15 Million*. Columbia Journalism Review. https://www.cjr.org/the_news_frontier/aol_settled_with_unpaid_volunt.php
58. Koivunen, A., Kyrölä, K., & Ryberg, I. (2018). Vulnerability as a political language. In A. Koivunen, K. Kyrölä, & I. Ryberg (Eds.), *The power of vulnerability*. Manchester University Press. doi: <https://doi.org/10.7765/9781526133113.00005>
59. Lacey, N. (1998). *Unspeakable Subjects: Feminist Essays in Legal and Social Theory*. Hart Publishing. doi: <https://doi.org/10.5040/9781472561916>
60. Levy, J., & Romo-Avilés, N. (2019). “A good little tool to get to know yourself a bit better”: A qualitative study on users’ experiences of app-supported menstrual tracking in Europe. *BMC Public Health*, 19(1), 1213. doi: <https://doi.org/10.1186/s12889-019-7549-8>
61. Lupton, D. (2015a). ‘Mastering Your Fertility’: The Digitised Reproductive Citizen. In A. McCosker, S. Vivienne, & A. Johns (Eds.), *Negotiating Digital Citizenship: Control, Contest and Culture*. Rowman & Littlefield Publishers. ISBN: 978-1-78348-889-6
62. Lupton, D. (2015b). Quantified sex: A critical analysis of sexual and reproductive self-tracking using apps. *Culture, Health & Sexuality*, 17(4), 440–453. doi: <https://doi.org/10.1080/13691058.2014.920528>
63. Lupton, D. (2016). *The quantified self: A sociology of self-tracking*. Polity. ISBN: 978-1-5095-0060-4
64. Malgieri, G., & Niklas, J. (2020). Vulnerable data subjects. *Computer Law & Security Review*, 37, 105415. doi: <https://doi.org/10.1016/j.clsr.2020.105415>
65. Marling, B. (2017, October 23). *Harvey Weinstein and the Economics of Consent*. The Atlantic. <https://www.theatlantic.com/entertainment/archive/2017/10/harvey-weinstein-and-the-economics-of-consent/543618/>
66. Marsden, C. (2018). Prosumer law and network platform regulation: The long view towards creating OffData. *Georgetown Law Technology Review*, 2(2), 376–398.
67. Marsh, S. (2018, May 1). Rise of contraceptive apps sparks fears over

- unwanted pregnancies. *The Guardian*. <http://www.theguardian.com/society/2018/may/01/rise-of-contraceptive-apps-sparks-fears-over-unwanted-pregnancies>
68. Moglia, M. L., Nguyen, H. V., Chyjek, K., Chen, K. T., & Castaño, P. M. (2016). Evaluation of Smartphone Menstrual Cycle Tracking Applications Using an Adapted APPLICATIONS Scoring System. *Obstetrics & Gynecology*, 127(6), 1153–1160. doi: <https://doi.org/10.1097/AOG.0000000000001444>
 69. Mosco, V. (2009). Chapter 7: Commodification: Content, Audiences, Labor. In *The Political Economy of Communication*. SAGE Publications Ltd. doi: <https://doi.org/10.4135/9781446279946>
 70. Mysoor, A. (2018, May 10). *How Women Can Use Monthly Periods As A Productivity Tool*. Forbes. <https://www.forbes.com/sites/alexandramysoor/2018/05/10/how-women-can-use-monthly-periods-as-a-productivity-tool/>
 71. Nardo, M., Manca, A., Rosati, R., & Loi, M. (2011). *The consumer empowerment index—A measure of skills, awareness and engagement of European consumers* (JRC Scientific and Technical Reports EUR 24791 EN). Institute for the Protection and Security of the Citizen (Joint Research Centre). <https://op.europa.eu/en-GB/publication-detail/-/publication/52e0bbef-6e82-49c5-a969-c50fdd98da6d/language-en>
 72. Palus, S. (2019, September 17). *There's One Good Reason to Share Period App Data: Medical Research*. Slate Magazine. <https://slate.com/technology/2019/09/period-apps-privacy-researchers-menstrual-pain.html>
 73. Peña, P., & Varon, J. (2019). *Consent to our Data Bodies: Lessons from feminist theories to enforce data protection*. CODING RIGHTS. <https://www.codingrights.org/docs/ConsentToOurDataBodies.pdf>
 74. Persdotter, J. (2020). Introducing Menstrunormativity: Toward a Complex Understanding of 'Menstrual Monsterings'. In C. Bobel, I. T. Winkler, B. Fahs, K. A. Hasson, E. A. Kissling, & T.-A. Roberts (Eds.), *The Palgrave Handbook of Critical Menstruation Studies* (pp. 357–373). Springer. doi: https://doi.org/10.1007/978-981-15-0614-7_29
 75. Privacy International. (2018). *How Apps on Android Share Data with Facebook*. <https://privacyinternational.org/sites/default/files/2018-12/How%20Apps%20on%20Android%20Share%20Data%20with%20Facebook%20-%20Privacy%20International.pdf>
 76. Privacy International. (2019, September 9). *No Body's Business But Mine: How Menstruation Apps Are Sharing Your Data*. Privacy International. <http://www.privacyinternational.org/long-read/3196/no-bodys-business-mine-how-menstruations-apps-are-sharing-your-data>
 77. Ptak, L. (2014, January). *Wages For Facebook*. Wages For Facebook. <http://wagesforfacebook.com/>
 78. Resta, G., & Zeno-Zencovich, V. (2018). Volontà e consenso nella fruizione dei servizi in rete. *Rivista Trimestrale Di Diritto e Procedura Civile*, LXXII(2), 411–440. ISSN 0391-1896
 79. Quintin, C. (2017). *The Pregnancy Panopticon*. Electronic Frontier Foundation. <https://www.eff.org/wp/pregnancy-panopticon>
 80. Regulation (EU) 2016/679 of the European Parliament and of the Council

- of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 32016R0679, European Parliament, Council of the European Union, OJ L 119 (2016). <http://data.europa.eu/eli/reg/2016/679/oj/eng>
81. Rosas, C. (2019). The Future is Femtech: Privacy and Data Security Issues Surrounding Femtech Applications. *Hastings Business Law Journal*, 15(2), 25. ISSN: 1554-8503
 82. Salleh, A., & Taylor, T. (2019, September 17). How effective is your fertility-tracker app? The numbers don't look good. *ABC News*. <https://www.abc.net.au/news/health/2019-09-17/fertility-ovulation-apps-half-ineffective-study-finds/11520074>
 83. Saner, E. (2019, July 10). *How period tracking can give all female athletes an edge*. The Guardian. <http://www.theguardian.com/lifeandstyle/shortcuts/2019/jul/10/how-period-tracking-can-give-all-female-athletes-an-edge>
 84. Schechner, S., & Secada, M. (2019, February 22). You Give Apps Sensitive Personal Information. Then They Tell Facebook. *Wall Street Journal*. <https://www.wsj.com/articles/you-give-apps-sensitive-personal-information-then-they-tell-facebook-11550851636>
 85. Silbaugh, K. (1997). COMMODIFICATION AND WOMEN'S HOUSEHOLD LABOR. *Yale Journal of Law & Feminism*, 9(1). <https://digitalcommons.law.yale.edu/yjlf/vol9/iss1/7>
 86. Solove, D. J. (2008). Understanding privacy. Cambridge: Harvard University Press. ISBN: 978-0-674-02772-5
 87. Soro, A. (2019, May 7). *Relazione sull'attività 2018. Discorso del Presidente Antonello Soro*. Garante Privacy. <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9109075>
 88. Statista. (September 14, 2020). Most popular types of purchased health apps in the U.S. as of 2020 [Graph]. In *Statista*. Retrieved April 25, 2021, from <https://www-statista-com.kuleuven.ezproxy.kuleuven.be/forecasts/1181559/share-of-health-apps-purchased-by-americans-by-type>
 89. Stepanov, I. (2020). Introducing a property right over data in the EU: The data producer's right – an evaluation. *International Review of Law, Computers & Technology*, 34(1), 65–86. doi: <https://doi.org/10.1080/13600869.2019.1631621>
 90. 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. doi: <https://doi.org/10.6035/Recerca.2019.24.2.9>
 91. Terranova, T. (2000). Free Labor: Producing Culture for the Digital Economy. *Social Text*, 18(2), 33–58. ISSN: 1527-1951
 92. The VOICE Group. (2010). Buying into motherhood? Problematic consumption and ambivalence in transitional phases. *Consumption Markets & Culture*, 13(4), 373–397. doi: <https://doi.org/10.1080/10253866.2010.502414>
 93. Tiffany, K. (2018, November 13). Period-tracking apps are not for women.

- Vox. <https://www.vox.com/the-goods/2018/11/13/18079458/menstrual-tracking-surveillance-glow-clue-apple-health>
94. Toffler, A. (1980). *The Third Wave*. William Morrow. ISBN: 9780688035976
 95. Vedder, A. (2018). Why data protection and transparency are not enough when facing social problems of machine learning in a big data context. In E. Bayamlioglu, I. Baraliuc, L. Janssens, & M. Hildebrandt (Eds.), *Being profiled: Cogitas ergo sum* (pp. 42–45). Amsterdam University Press. doi: <https://doi.org/10.5117/9789463722124>
 96. Verhenneman, G. (2020). *The patient's right to privacy and autonomy against a changing healthcare model—Assessing informed consent, anonymisation and purpose limitation in light of e-health and personalised healthcare*. [PhD Thesis]. KU Leuven.
 97. Viljoen, S. (2020). Democratic Data: A Relational Theory For Data Governance. SSRN Electronic Journal. doi: <https://doi.org/10.2139/ssrn.3727562>
 98. Wachanga. (2020, January 23). *Privacy Policy*. Wachanga. <https://wachanga.com/en/privacy>
 99. Weigel, M. (2016, March 23). 'Fitbit for your period': The rise of fertility tracking | Moira Weigel. *The Guardian*. <http://www.theguardian.com/technology/2016/mar/23/fitbit-for-your-period-the-rise-of-fertility-tracking>
 100. Wittkower, D. E. (2016). Lurkers, creepers, and virtuous interactivity: From property rights to consent and care as a conceptual basis for privacy concerns and information ethics. *First Monday*. doi: <https://doi.org/10.5210/fm.v21i10.6948>
 101. WomanLog. (2019, November 19). *Privacy policy*. WomanLog. https://www.womanlog.com/privacy_policy
 102. Zech, H. (2017). Data as a Tradeable Commodity – Implications for Contract Law. *SSRN Electronic Journal*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3063153

Acknowledgments

The authors would like to thank Renate Baumgartner, Kylie Jarrett and the special issue editors for very helpful comments and suggestions. All remaining errors are the authors' responsibility.

Appendix

TABLE 1: Types of data whose processing is explicitly mentioned in the privacy policies of six popular FMTs

	APP NAME	FLO	CLUE	CLOVER	PERIOD TRACKER DELUXE	PERIOD DIARY PRO	WOMANLOG
ACCOUNT DATA	Name/ Username/ Nickname	x	x	x		x	
	Email address	x	x	x	x	x	x
	Gender	x		x			
	Date of birth	x		x		x	
	Password/ passcode	x		x		x	
	Location	x		x		x	x
	ID number	x					
	Picture			x			
	Phone number			x		x	
	Time zone	x		x			
	Service preferences			x			
	Identifiers	x	x	x	x	x	
	Company					x	
	Purchasing/ transaction data					x	
	Language						x
HEALTH DATA	Body measurements	x	x	x		x	x
	Body temperature	x	x	x			
	Menstrual cycle dates	x	x	x		x	x

	Various symptoms	x	x	x			x
	Other information about health, wellbeing and activities	x	x	x			
	Health goals			x		x	
	Health-related information about child			x			
	Pregnancy-related information					x	
DEVICE DATA	Hardware model	x	x	x	x	x	x
	Operating system	x		x	x		x
	Unique device identifiers	x	x	x	x	x	
	Mobile network information	x					
	Device storage information	x					
	Device settings		x				
	Application identifier		x				
	Crash information		x				
	Browser		x	x			
	Browser settings		x				
	Manufacturer			x			

	MAC address			x			
	Time-stamped logs of messages sent and received			x			
	Network status			x			
	Screen information			x			
	Mobile service provider	x		x			
	Installed app version			x			
	Applications installed in a mobile device					x	
APP USAGE DATA	Frequency of use	x					
	General activity	x	x		x	x	x
	Engagement with particular features/ services	x					x
	Acquisition channel / exit URLs					x	x
	Authentication						x
	Notification activity						
OTHER	User content			x			
	Communications			x		x	
	Survey					x	

	responses						
	Third-party information (e.g., from Apple HealthKit, Google Fit, Facebook, Twitter, Instagram)	x		x		x	x

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