Feminist Legal Studies
https://doi.org/10.1007/s10691-021-09486-y

Rethinking Explicit Consent and Intimate Data: The Case of Menstruapps

Daniela Alaattinoğlu[1,2]

Accepted: 20 December 2021

Abstract
Period-tracking software applications or 'menstruapps' have witnessed a surge in popularity in recent years. At the same time, many of them are a part of the adtech industry, using business models that create revenue by selling users' personal and intimate data. This exploratory article brings menstruapps into a feminist legal debate. It investigates the supranational European legal standards on intimate and sensitive data processing, particularly the General Data Protection Regulation (GDPR). Scrutinising explicit consent according to GDPR Article 9, this paper, through empirical examples, claims that current legal standards are not enforced. The standards are, furthermore, theoretically insufficient to fully safeguard data subjects' integrity and autonomy. Instead of abandoning the concept, the article reimagines consent, using a contextual and communicative model where power relations are taken into consideration, building on the feminist concept of *freedom to negotiate*.

Keywords Consent · Explicit consent · GDPR · Intimate data · Menstruapps

Period-Tracking as Increased Bodily Control—But by and for Whom?

In the age of surveillance capitalism and the quantified self, constantly developing technology is increasingly collecting and sharing data about our lives, for example by observing, measuring and evaluating our bodies, physical fitness and health (see Daly 2015; Leibenger et al. 2016; Parker et al. 2017). Among such health-related measuring gadgets are the highly popular menstruation, fertility and pregnancy software applications ('menstruapps' and 'period-tracking apps'). These apps provide

✉ Daniela Alaattinoğlu
daniela@hi.is

[1] Icelandic Research Fund Postdoctoral Researcher, Faculty of Law, University of Iceland, Sæmundargata 2, 102 Reykjavík, Iceland

[2] Faculty of Law, University of Turku, Caloniankuja 3, 20014 Turku, Finland

Published online: 04 March 2022

data-driven, modern services to self-track periods—a practice which in itself predates modernity—to monitor and control reproductive and sexual health.[1]

Menstruapps gather extremely sensitive data, often on topics beyond periods—such as sexual intercourse and positions, masturbation, orgasms, use of emergency contraception, sleep, stress levels, physical symptoms, moods or vaginal discharge. Sometimes the software apps are accompanied by hardware appliances, such as ovulation tests, thermometers or menstruation cups using Bluetooth technology, further emphasising the intimate nature of the data processed (Rizk and Othman 2016). Reports on the data collected through the apps, often stored in the cloud (see Leibenger et al. 2016, 317), can be shared with third parties, for example, partners, healthcare providers or researchers. Many menstruapps also share data with advertisers. The legal ground for intimate and sensitive data processing[2] used by menstruapps is, as a rule, their users' consent.

With users giving consent for menstruapps to process their personal data,[3] the apps, in turn, often use scientific, empowering and even feminist language to appeal to customers. "Reclaim your month", "run your world" (MyFloTracker 2020), "for women who want to take control of their health and sex lives" (App Store 2020), and "be the girl in your class who understands her body" (MagicGirl 2020) are examples of the rhetoric used by popular menstruapps. In these examples, menstruation is viewed as a deficit to be controlled or suppressed, a reproductive problem to be managed through the accumulation of information, the victory of the mind over the rebellious body (see Federici 2014). Simultaneously, the popularity and growing markets of menstruapps dovetail with feminist and human rights mainstreaming efforts at breaking stigmas and disinformation connected to periods and reproductive and sexual health (see, for example, UN Women 2019).[4] Furthermore, their popularity also coincides with efforts to address the existing gender data gap.[5] Hence, menstruapps place themselves in the peculiar intersection between feminist mainstreaming of public debate and the capitalist search for new products and markets—a place where the inefficient, menstruating body ought to be disciplined.

[1] An aim which is, ultimately, beyond human control. On the gendered control over reproductive and sexual bodies and its intimate connection to modern capitalism, see Federici (2014).

[2] In this article, data processing is understood in line with GDPR art 4(2):

[…] any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

[3] Personal data, according to GDPR art 4(1), means:

[…] any information relating to an identified or identifiable natural person […]; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

[4] This relationship can be depicted both as symbiotic, on the one hand, and as capitalist appropriation of feminist and human rights agendas, on the other. The tandem is not, however, a "mere coincidence", but rather, a "perverse, subterranean elective affinity" (Fraser 2013, 218).

[5] In other words, the domination of collected data based on studies of men, rather than women, and the deficit of data relating to women and areas typically viewed as 'feminine'. See Criado Perez (2019).

By offering an accessible way of self-tracking periods on our ubiquitous handheld devices, menstruapps answer the needs of many people who menstruate (for example, cis women, trans men or non-binary people) to better understand the regularities and irregularities of the menstrual cycle. Apart from aiding their users, the apps also provide scientific opportunities for increased data on menstrual cycles, improving the understanding of menstrual health (Li et al. 2020). The apps, nevertheless, through the creation of revenue by selling individuals' intimate data, feed into a long tradition of measuring and standardising, medicalising and monetising menstruation and gendered bodies (see Federici 2014; Lupton 2015).

Despite their gendered exploitation of intimate data and their inherent data privacy concerns (see Daly 2015; Leibenger et al. 2016), menstruapps have been remarkably under-researched and under-critiqued in the emerging mainstreaming of data privacy as a fundamental right. This article bridges the existing disciplinary gap between legal discussions on data privacy and consent, critical analysis of menstrual health tracking and feminist legal theory. Moreover, it originally interrogates the European Union (EU) special legal standard of 'explicit consent' pertaining to processing sensitive and intimate data, a standard which is rarely distinguished from regular consent. The text, importantly, brings menstruapps into a feminist legal discussion by investigating their privacy policies. It is the first scholarly contribution that theoretically and empirically scrutinises the gendered and intersectional exploitation for profit at play in menstruapps and reimagines the current legal standards by using the feminist concept of *freedom to negotiate*. As such, the article is an example of how feminist theory can be used to develop the current legal standards of ethical data processing.

In the following section, the article interrogates the European legal standards on sensitive data protection, particularly explicit consent, laid down in the General Data Protection Regulation (GDPR) 2016/679, Article 9. It does so by drawing on three analytical axes: context, power and communication. In the third section, looking closer at seven popular menstruapps, the article empirically investigates whether users' explicit consent is obtained, what their consent choices look like and how their agency is formulated. In its final two sections, the article reimagines current supranational legal standards, which now operate around a binary yes/no model, in a contextual model that concentrates on the role of the data controllers, the power imbalance between the contractual parties, the personal experiences of data subjects and their limited power of negotiation.

Menstruapps and Consent

Menstruapps are one feature of the emerging market of collecting and selling the digital-age currency of personal data. The increasing commodification of personal data, a market dominated by a few major players, is a growing global concern for

human rights and privacy advocates (see Daly 2016).[6] The adtech industry, particularly through software apps, collects and creates profiles of users and distributes such information to third parties, sometimes without consumers' knowledge or consent. Other times, the only way for individuals to access the services of an app is by agreeing to personal data sharing (see Forbrukerrådet 2020). This market is particularly worrying as many people share their highly intimate data with a sense of trust and confidence.[7] The use of consent in menstruapps has been criticised for its opaqueness (see, for example, Privacy International 2019). Market-leading menstruapps nevertheless continue to create revenue by exploiting their users' unpaid work by monitoring their reproductive cycles and fertility. Such capitalist, gendered exploitation "must be considered in light of the historic lack of recognition for women's sexual, reproductive and relational labor" (Coding Rights 2016).

The encounter between the data subject—the "identified or identifiable natural person" (GDPR Article 4(1))—on the one hand, and the data controller—the natural or legal person that determines "the purposes and means" of the data processing (GDPR Article 4(7) —on the other, is often thought of as a contractual exchange. Accordingly, the data subject seeks to access a service and consents to her data being processed and shared. When it comes to processing personal data, consent is legally considered a valid contractual ground in many countries.[8] Such a regulation of data privacy individualises responsibility, decentring the necessity for institutional safeguards for ethical data processing (see, for example, Koops 2014; Mantelero 2014; Cohen 2019). Consent here risks becoming a "free-standing justificatory standard" (Brownsword 2004, 226) that "legitimizes nearly any form of collection, use or disclosure of personal data" (Solove 2013, 1880): a symptom of a legal culture which overemphasises the liberal ideal of the autonomous individual and presupposes her agency. Legal standards envisioned to protect the autonomy of individuals when engaging in such contractual relationships should therefore be interrogated for their inability to problematise the underlying assumptions which might, in turn, undermine the same individuals' free choice.

Feminist theory here offers alternative ways of thinking about consent. Feminist theorists have criticised the liberal premises underlying the legal construction of the independent legal subject and the consent/non-consent dyad for decades (see, for example, Pateman 1980; Kazan 1998; Ahmed 2017). Carol Smart, writing on the legal standards surrounding rape in England, has criticised the pair of opposites

[6] In its 2019 report on Facebook and Google, Amnesty International criticised how people are "only able to enjoy their human rights online by submitting to a system predicated on human rights abuse" (Amnesty International 2019, 5).

[7] On the inappropriate sharing of personal data, i.e. disregarding contextual social norms, as a major privacy concern, see Nissenbaum (2009).

[8] In the context of the United States of America (US), for example, the notice-and-consent and duty-to-read doctrines (see Benoliel and Becher 2019) of privacy policies they subsequently agree to remain the "fallback approach in online privacy policies" (Nissenbaum 2011, 32). Privacy policies and consent processes nevertheless often run the risk of becoming "box-ticking exercises that aim to limit" data controllers' legal liability, rather than being concerned with consumers' possibilities to protect their privacy (Parker et al. 2017, 10).

(consent or non-consent) for failing to take into consideration the complexity of choice and its underlying coercive conditions (Smart 1989, 33–34). Furthermore, Tanya Palmer has critiqued the ambiguity of consent in the Sexual Offences Act 2003 as a dividing line between criminalised and non-criminalised sexual behaviour. She suggests that we rethink current standards of consent through the concept of freedom to negotiate (Palmer 2013, 2017).[9]

The abstract concept of consent builds on the presence or absence of an agreement. Palmer particularly points out the inability to incorporate *context* in this abstract notion since, in human interactions, there is a practical lack of agreed definitions of consent. Rather than classifying sexual encounters as strictly consensual or non-consensual, Palmer suggests that the context in which sexual agreements are made should be given higher importance. Palmer proposes that we investigate whether people are free to say no and whether they have an equal say in what kinds of sexual activity takes place—focusing on who has the *power* to set the terms of such agreements (Palmer 2013, 5). Palmer also emphasises the need for open discussion and *communication* (Palmer 2013, 3) when conceptualising sexual violence, based on her analysis of a series of interviews and focus groups with laypeople, police officers, domestic violence support workers and caseworkers. These three analytical lenses—context, power and communication—can also create a theoretical framework for a feminist reappropriation of consent in relation to menstruapps.

Context: The Neoliberal, International Market and Developing European Law

Menstruapps are created for the global market. They are often available in English, alternatively translated, more or less understandably, into several languages. As such, they constitute an attempt at standardising a period-tracking tool for a diversity of data subjects in various nations, accessing the applications in varying material conditions, using their different (and possibly limited) linguistic and technical skills, in differing cultural, ethnic and socio-economic conditions, with disparate knowledge, abilities and interests regarding reproductive and sexual health.

Against this reality that promises individuals control and understanding of their bodies, the popularity of the apps is not explained merely by personal preferences of increasingly data-conscious users. Rather, popular apps ought to be put into the context of a world where public health services, particularly pertaining to sexual and reproductive health, face austerity measures and the management and responsibility of health and fertility are increasingly placed on the individual.[10] Utopianly promising a technological answer to a range of political and medical problems, such as infertility, menstruapps provide "technologically aided assurance in place of medical attention" (Fox and Epstein 2020, 735). Such developments might make the apps particularly attractive to people who menstruate and whose material access

[9] Earlier feminist accounts analysing negotiation in connection to consent are crucial for Palmer's contribution. See, importantly, Anderson (2004).

[10] An illustrative example is the 'home' smear tests offered by the National Health Service (NHS) in the United Kingdom; see NHS (2021).

to reproductive health information and services is restricted, for example due to limited financial means or insufficient public healthcare services. Legal data privacy standards and their enforcement also vary considerably between different countries, creating another layer of inequality. When data subjects only need a smartphone and an internet connection, it is easy for data controllers to turn their menstruation into money by selling their intimate data.

Menstruapps, like other software applications, are also a phenomenon that cuts across several traditional jurisdictions and legal areas. Such apps are often developed on behalf of a company based in one or multiple countries, and used by people in the same, or other, countries. The global reach of the apps raises legal questions relating to jurisdiction and liability, as most legal systems still build on the idea of the nation state. European—and particularly EU—data protection law is here an internationally cutting-edge attempt at creating a supranational regulation system for data processing. Importantly, regardless of the data controllers' countries of origin, the GDPR is applicable for all personal data processing concerning data subjects located within the European Union (Article 3 GDPR).[11]

European data protection law has advanced guiding legal principles for data subjects' consent regarding personal and intimate data. One such principle is the right to protection of the data subject against unlimited processing of personal data—the right to "informational self-determination" (see Rouvroy and Poullet 2009).[12] In principle, the right guarantees the authority of individuals to decide on the processing of their personal data.

The idea of individuals as self-determined players who can consent to or refuse data processing is also present in the interpretation of the 1950 European Convention on Human Rights and Fundamental Freedoms (ECHR, the Convention) by the European Court of Human Rights (ECtHR). The right to informational self-determination has primarily been conceptualised as inherent in the right to respect for private and family life (Article 8). In general, the Court has considered that the right protects individuals' personal information—such as DNA, fingerprints, cellular samples, birth records, health records or photographs—from being processed without consent.[13] However, in some cases when individuals have not consented to the processing of personal data, restrictions of the right to respect for private and family life have been justified as motivated by public interest and falling within the margin of appreciation of the state.[14]

[11] Also the transfer of personal data to a third country must abide by the standards laid down in EU law. See CJEU case C-311/18 ('Schrems II'), EU:C:2020:559.

[12] This right to informational self-determination can ultimately be traced back to German constitutional jurisprudence (BVerfG, Judgment of the First Senate of 15 December 1983, 1 BvR 209, 269, 362, 420, 440, 484/483). In a report from 2019 by the German Data Ethics Commission (*Datenethikkommission*), the principle was restated as *digital* self-determination, meaning the idea "of a human being a self-determined player in a data society" (Datenethikkommission 2019, 6).

[13] See *Odièvre v France* [2003] App no 42326/98. *S and Marper v the United Kingdom* [2008] App nos 30562/04 and 30566/04. *YY v Russia* [2016] App no 40378/06. and *Bogomolova v Russia* [2017] App no 13812/09.

[14] See *Murray v the United Kingdom* [1994] App no 14310/88 and *GSB v Switzerland* [2015] App no 28601/11.

Despite the ECtHR's emerging rulings on data privacy, the epicentre of European data protection law is nevertheless not located in Strasbourg. In this field, the EU institutions have, as an aspect of consumer protection, for a considerable time paved the way (see Kosta 2013). Importantly, in the 2000 Charter of Fundamental Rights of the European Union, the respect for private and family life (Article 7) and the protection of personal data (Article 8) are regulated as separate rights.[15] According to Article 8, personal data "must be processed fairly for specified purposes and *on the basis of the consent of the person concerned* or some other legitimate basis laid down by law" (Article 8(2), author's emphasis). The Court of Justice of the European Union (CJEU) has also ruled on questions pertaining to consent and data protection. In its preliminary ruling C-40/17 ('Fashion ID'),[16] the CJEU stated that data subjects' consent must be obtained *prior* to the data collection (para 102). In the case C-673/17 ('Planet49'),[17] moreover, the same Court pointed out that consent to data processing cannot be "presumed but must be the result of active behaviour on the part of the user" (para 56).

Power: Sensitive Data and Explicit Consent in the GDPR

The EU flagship on data protection, the already-mentioned GDPR, contains more specific regulations on the legal basis for processing personal data.[18] Consent is, importantly, only one of them (Article 6(1)(a)).[19] The GDPR also specifies how valid consent to personal data processing is given (Articles 7 and 8). Consent, according to the definition in the GDPR, is a "*freely given*, *specific*, *informed* and *unambiguous* indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her" (Article 4(11), author's emphasis).

The conditions for consent to be valid are specified by the European Data Protection Board (EDPB). According to the EDPB, consent is freely given if the data subject has real choice and control (EDPB 2020, para 13). Accordingly, if consent is "bundled up as a non-negotiable part of terms and conditions it is presumed not to have been freely given" (para 13). The same applies when refusal or withdrawal of consent leads to negative consequences for the data subject (para 13). A freely given consent, according to the EDPB guidelines, should not involve an imbalance of power between the data subject and the data controller (paras 16–24). Moreover,

[15] On the protection of personal data as a fundamental right, see Gonzalez Fuster (2014), Lynskey (2014).

[16] EU:C:2019:629.

[17] EU:C:2019:801.

[18] The GDPR replaced the 1995 Data Protection Directive (95/46/EC).

[19] If processing is necessary, the other legal grounds are: for the performance of a contract, for compliance with legal obligations, to protect the vital interests of the data subject, to carry out a task in public interest or for the purposes of the legitimate interests under GDPR art 6(1). Special conditions apply to the consent of children under the age of 16. These are regulated under GDPR art 8.

it should be unconditional (paras 25–41), granular (paras 42–45) and without detriment to the data subject (paras 46–54).

Valid consent in the GDPR must also be specific, which according to the EDPB means that the data subject consents separately in relation to the particular purposes of the data processing (paras 55–61). When it comes to the consent being informed, the EDPB guidelines highlight that information should be provided to data subjects before their giving consent. Moreover, it is important that subjects can understand what they agree to and that they can withdraw their consent (paras 62–74). When it comes to the final requirement of unambiguity, it is required that consent should always be given through a "clear affirmative act" (para 75; affirmed by the CJEU in case C-673/17 ['Planet49']). Hence, the data subject's silence or passivity cannot be interpreted as a sign of acceptance (para 79). A general acceptance of terms and conditions is, moreover, not a valid form of consent for the processing of personal data (para 81). In general, the regulation of regular consent in the GDPR draws up the minimum requirements for the responsibility of the data controller to inform the data subject and obtain, rather than assume, their consent. Simultaneously, it builds on the notion of the controlled, the data subject, as a well-informed consumer who can make a free and informed decision on whether their personal data can be processed or not.

When it comes to menstruapps, however, the data processed specifically relates to the reproductive and sexual health of their users. Such intimate and particularly sensitive data fall within the 'special categories of personal data' regulated in GDPR Article 9, which, according to the main rule, must not be processed.[20] The most important ground, and likely the only one applicable for menstruapps, for exceptionally processing such data is, nevertheless, the 'explicit consent' by the data subject [Article 9(2)(a)].[21]

How the validity of explicit consent normatively differs from that of regular consent in communication, form and content is not—interestingly—specified in the GDPR. Further guidance is nevertheless provided by the EDPB. According to the guidelines, the term *explicit* "refers to the way consent is expressed by the data subject", calling for an "express statement of consent" (EDPB 2020, para 93). The data controller can, for example, obtain such explicit consent by requiring the user to sign a written statement, fill in an electronic form, send an email, upload a scanned document with the data subject's signature, use an electronic signature, give an oral statement, through a telephone conversation or a two-stage verification (paras. 94–98).

[20] According to GDPR art 9(1):
Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

[21] The other exceptions are listed under GDPR art 9(2–3) and are, for example, "when processing is necessary to protect the vital interests of the data subject or another natural person" (2)(c); when processing relates to data "manifestly made public by the data subject" (2)(e); when "processing is necessary for reasons of substantial public interest" (2)(g); or when it is "necessary for the purposes of preventive or occupational medicine" under certain circumstances (2)(h)(3).

The information about the choice, particularly if explicit consent is obtained through a telephone conversation, should be "fair, intelligible and clear" (para 95). Therefore, the guidelines provide an open-ended list of forms through which such explicit consent can be obtained. However, they do not contain specific regulations on the normative content of explicit consent in comparison to regular consent. This void leads to the conclusion that the normative *content* regulation of the elements of valid consent is similar for the two, but the *form* is further pronounced when the personal data belong to protected special categories.[22] Hence, the imagined legal roles of the data controller and the data subject also remain similar when very intimate data is processed, even though the power dynamics at play might be different, in comparison to the processing of other data.

One can ask whether, and under what circumstances, data subjects, in reality, can give consent in a way that is free, specific, informed and unambiguous. In fact, the choice to consent always already involves social, commercial and financial pressure, and the complexity of data processing also makes informed choices practically impossible (Nissenbaum 2011, 35–36). There is a power imbalance between data subjects and controllers, individual consumers and companies (see Daly 2016). Data subjects, according to Paz Peña and Joana Varon, "are deprived of "no" when [facing an] ... oversimplified binary option between agree or disagree, while the latest ultimately means opting for some level of digital exclusion" (Peña and Varon 2019, 13).

The power dynamics at play, especially when referring to menstruapps, is also gendered and intersectional: the intimate data exploited by the controllers relate to the "identified" or "identifiable" (GDPR Art. 4(1)) physical and data bodies that bleed, ache, discharge and orgasm. The identities and bodies of the data controllers, on the other hand, controlling, exploiting and selling the data—remain largely anonymous, non-embodied, abstract and blurred.

Apart from the question of the validity of data subjects' consent to sharing intimate personal data, one can also ask what normative control the programmers, app developers and companies trading intimate data exercise over menstruating bodies. This question goes beyond exploitation of personal data, as the software applications also tend to create stereotypical, medicalised and exclusionary imagery of menstruation bleeding and the bodies that bleed—exemplified by standardised (and often incorrect) period prediction,[23] or stereotypically pink graphical user interfaces (see Epstein et al. 2017; Fox and Epstein 2020, 737–740). Menstruapps, moreover, often use cisnormative assumptions about users and equally heteronormative presumptions about their partners.

[22] The lack of specific guidelines on the content and form of explicit consent leads to differences in national interpretation of the GDPR. The British Information Commissioner's Office, for example, considers ticking a box enough to fulfil the formal requirements for explicit consent. The Finnish Office of the Data Protection Ombudsman, on the other hand, does not consider ticking a box to be enough. See Information Commissioner's Office (2020), Office of the Data Protection Ombudsman (2020).

[23] The standardisation of the 'regular' menstrual cycle is a modern phenomenon, dominated by western-centred medicine. This is particularly true since the reproductive age, together with lengths, experiences and cultural standing of periods vary across the world. In the words of Lahiri-Dutt, "menstruation was an irregular and infrequent occurrence among most women until recently" (Lahiri-Dutt 2015, 1161).

By documenting the menstrual cycle and promoting planned pregnancy, giving users cues for how to make responsible reproductive choices, menstruapps medicalise the reproductive cycle and gendered bodies (Lupton 2015, 447). In a neoliberal setting, where individual responsibility for health is highlighted, such apps become normative and disciplinary, "working to tame the sexual and reproductive body by rendering it amenable to monitoring, tracking and detailed analysis of the data thus generated, and producing ever-more-detailed categories of behaviour" (Lupton 2015, 449). Furthermore, as a disciplinary practice, menstruapps create a modern tool to manage the bleeding body, fed by "the economic urgency to present" all bodies as "labouring" and to make this appear "natural and normative" (Lahiri-Dutt 2015, 1162).

The oxymoron present in the promise of emancipation through detailed observation, knowledge and mastery of the reproductive and sexual body (see Young 2005, 101–102) is an interesting trait of menstruapps. Through minute observation, tracking and reporting the menstrual cycle, users ultimately gain 'emancipatory' sexual and reproductive knowledge—control of their bodies. Simultaneously, the presumed purpose of such managerial skills is, paradoxically, imitating a non-bleeding, presumed male or invisibly gendered, efficient norm—concealing the inefficient, bleeding and visibly gendered body (see Young 2005, 106–110). This feeds into the general "split subjectivity" of people who menstruate, claiming normalcy, on the one hand, and fearing the "private fluidity" of the flesh, on the other (Young 2005, 110).

Communication: Respecting the Desires of Data Subjects

Imagining agreements where menstruapp users have decisive power beyond saying 'yes' or 'no', the freedom to negotiate inspires (Palmer 2013). The concept aims at the communication between the parties to discuss and determine the terms of the agreement. In the context of software apps, communication means the possibilities for data subjects to affect the terms of agreements and possibilities to communicate their desires, wishes and concerns to the data controllers. An underlying assumption is for such desires to be respected by the data controllers.

For a developed view on communication as a legal standard, further guidance can be found in bioethics. Communication is today seen as a core part of professional medicine—ideally, a means to guarantee that the patient can make an informed and free decision—guided by the principle of protecting the patient's autonomy (Schaper and Schicktanz 2018, 3). Looking at direct-to-consumer genetic testing services, Manuel Schaper and Silke Schicktanz contend that the standards guiding communication are starkly different in medicine (informing, respecting the autonomy of the patient) versus advertising (consumer persuasion to increase sales) (Schaper and Schicktanz 2018, 3–4). Analogies between genetic testing services and period-tracking applications can be made, since both rest on the tense intersection between medicine and the market, where the logics of the latter tend to dominate communication. As such, menstruapps inherently pose ethical problems—especially as it may be difficult for the public to navigate the complex, multimodal communication on the

digital market when companies utilise the sense of legitimacy and trust commonly associated with medicine for advertising purposes (Schaper and Schicktanz 2018, 9).

Communication is nevertheless always already affected by the other two axes of the analysis: context and power. Liz Brosnan and Eilionóir Flynn, in the context of rights for people with disabilities, contend that a 'mere agreement' should not be regarded as evidence of free and informed consent (Brosnan and Flynn 2017, 65). They argue that there ought to be an active communicative process between contractual parties to reach an agreement (Brosnan and Flynn 2017, 65). Ideally, all forms of coercion, undue influence and power imbalances should be eliminated from or minimised in such communication (Brosnan and Flynn 2017, 69–70). A first step for doing so is to recognise overt, covert and hegemonic power (Brosnan and Flynn 2017, 72). The abilities of menstruapp users to freely communicate—in a way that is intelligible, recognised and respected by the data controllers—thus depend, for example, on their technical knowledge, awareness of their legal rights as data subjects, linguistic abilities, financial, social and cultural resources or modes of communication.

Formulations of Explicit Consent in Menstruapps

Rather than providing a comprehensive overview of the constantly emerging and developing menstruapps available, this section investigates—in a limited, non-representative way—some of the most popular apps on the market and their conceptualisation of consent and user agency. The apps investigated are free of charge and have more than one million downloads through Google Play Store.[24] The seven apps investigated—the majority of them owned by companies located outside of the European Union[25]—are as follows: Clue by BioWink, Period Tracker by Simple Design Ltd., Flo:Period Tracker by Flo Health, Period Tracker by Leap Fitness Group, Period Tracker by GP International LLC, Period Calendar, Cycle Tracker by SimpleInnovation and Period Tracker by Amila.[26] The GDPR is applicable for all these menstruapps (Article 3 GDPR). The documents particularly scrutinised were their privacy policies as of July 2020.[27] The apps have also been downloaded and used by the author in the same time period.

[24] Not investigating other app stores is one limitation of the study that affects its ability to make representative claims.

[25] The headquarters of the companies are in Germany (BioWink), the British Virgin Islands (Simple Design), the US (Flo Health, GP International LLC and SimpleInnovation), Singapore (Leap Fitness Group) and Cyprus (Amila).

[26] Only Clue by BioWink requires registration. This does not, however, have an impact on the data processed.

[27] Studying privacy policies and terms and conditions is one possible way of investigating software apps' data and privacy protection. See Sunyaev et al. (2015), O'Laughlin et al. (2019), Jia and Ruan (2020).

The privacy policies specified the user data collected in different ways. Often, the documents formulated the type of processed data in general and vague terms. The period trackers by Simple Design Ltd. and Leap Fitness Group claimed not to generally collect "personal identifiable information" when the user downloaded the app, not specifying or exemplifying what this information may be (Simple Design 2020; Leap 2020). While the meaning of such statements is vague and does not correspond to the terminology used in the GDPR,[28] it is worth pointing out that even if the data undergo anonymisation, such processes do not answer the question of what kinds of personal data are processed in the first place. SimpleInnovation, for example, vaguely stated that the information automatically collected through their menstruapp "may include usage details, metadata, and real-time information about the location of your device" (SimpleInnovation 2019, 1). GP International LLC's period tracker similarly processed *at least* device data, event and usage data and the user's IP address (GP Apps 2020). Remarkably, the only menstruapps specifying that they process health and sensitive data—which, in fact, all of them do—were those provided by Biowink, Flo Health and Amila (Amila 2019; Clue 2020; Flo Health 2020). Their privacy policies were also the most specific concerning the types of data collected. Biowink's app, for example, stated that, "We store health data, such as your body measurements, dates of your past and current periods, and symptoms or events you choose to track in the app (e.g. sex, levels of productivity, good hair days, pain, or cravings) (Clue 2020)."

For processing personal data, as pointed out earlier, consent is not the only possible legal basis according to the GDPR. All the privacy policies investigated nevertheless legally based data processing on consent or even, in some cases, explicit consent. The only app that refers to the GDPR specifically was Clue by Biowink.[29] Flo Health's period tracker, for example, stated that it (Table 1).

> […] will not process Personal Data in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by you or collect any Personal Data that is not needed for the mentioned purposes. For any *new* purpose of processing we will ask your *separate explicit consent* (Flo Health 2020, author's emphasis).

When downloading and starting to use menstruapps, the data subject ought to consent to personal data processing. Remarkably, only four of the seven apps explicitly asked for users' consent at the outset. Clue by Biowink, for example, asked the user to agree to its privacy policy to sign up to use the app. Yet the user was only given one option, which was to agree to the privacy policy in its entirety. Flo:Period

[28] It may nevertheless have a more specific meaning in other jurisdictions (such as some US states). Yet, there were no references to jurisdiction in the privacy policies.

[29] Clue's privacy policy specifies that the company bases its data collection on art. 6 s 1(b) and 1(f) GDPR, art. 9, together with s 27 in the German Data Protection Act (Clue 2020).

Tracker, in turn, specifically asked for consent to process personal health data on the registration screen. SimpleInnovation and Amila's menstruapps asked for consent to process personal data when opening the app. SimpleInnovation here provided two options, "yes, I agree" and "no, thank you" (Simple Innovation 2019), while Amila's only option was to agree. In three of the menstruapps, on the other hand, consent was not requested, but assumed through a pre-ticked box (Simple Design Ltd. and Leap Fitness Group's apps) or when creating an account (GP International LLC's app). Users' consent at the outset was not always specifically asked for. Moreover, when the data subject's consent was specifically obtained at the outset, consent was sometimes formulated as a bundled-up, wholesale yes/no choice to accept privacy policies and personal data processing. Facing such choices, data subjects have limited possibilities to use the app if they do not wish their personal data to be processed.

The possibility for retracting consent once provided is essential to the concept itself (Table 2). Data subjects may want to revoke their consent to future data processing (GDPR Article 7(3)), or to delete the personal user data that the apps have already collected (see GDPR Article 17). As seen in the table above, the apps generally provide possibilities for consent to be revoked regarding the future collection of data and for collected data to be deleted. The only privacy statements that did not provide any information about whether collected personal data could be deleted were those of Simple Design Ltd. and Leap Fitness Group's period trackers (Simple Design 2020; Leap 2020). Nevertheless, these apps provided an in-app option to delete all data. In the cases of BioWink, Flo Health and SimpleInnovation's menstruapps, complete deletion of already-collected data could be done by emailing the companies (SimpleInnovation 2019; Clue 2020; Flo Health 2020). In Amila's period tracker, on the other hand, instructions for how to delete personal user data were not specifically given (Amila 2019).

In general, when the option to delete collected personal data was given, it often presumed that the user would also delete and no longer use the app. GP International LLC's period tracker, for example, stated that:

> If you'd like us to delete User Provided Data that you have provided via the Application, you may delete your account and associated data by going to the app settings, account page, and select delete account. This will delete your account and associated data from our servers. Deleting the native app on your phone will also delete any app data your phone holds (GP Apps 2020).

What remains unclear is whether users can continue to use the apps after consent to processing personal data has been revoked and/or personal data erased, or whether a refusal to consent equals digital exclusion. This question raises further inquiries about the possibility of consenting to the processing of personal data only in situations when the data subject sees fit.

When it comes to data subjects consenting to share their personal information with third parties, such as advertisers or analytics companies, the menstruapps compared provide different options. As stated earlier, one option—sometimes the only one—for users not to agree to share personal data with third parties was to reject the privacy policies in their entirety. Such a rejection, nevertheless, often affected users'

Table 1 Data subject's consent when starting to use the menstruapp

Menstruapp	Data subject actively consents to personal data processing at the outset
Clue (BioWink)	Yes, but bundled up with privacy policy
Period Tracker (Simple Design Ltd.)	No
Flo: Period Tracker (Flo Health)	Yes
Period Tracker (Leap Fitness Group)	No
Period Tracker (GP International LLC)	No
Period Calendar, Cycle Tracker (SimpleInnovation)	Yes
Period Tracker (Amila)	Yes, however only one option

ability to use the apps. In some cases, there were in-app options to limit information sharing to third parties, but no option to reject such data sharing completely (see, for example, GP Apps 2020). Apart from in-app options, some apps envisioned other ways for users to customise their consent to third-party data sharing. For example, in the case of BioWink's Clue, an app which shares information with third parties for scientific research purposes, users who do not feel "comfortable with [their] de-identified data being shared for the purposes of menstrual and reproductive health research" were encouraged to email the company (Clue 2020). In general, users' consent to third-party information sharing was assumed upon agreeing to data processing or, alternatively, the terms and conditions of the menstruapps. In addition to this, the identity of third parties—and their potential use of personal data—was often depicted in vague terms or even unspecified in the privacy policies.

In the context of menstruapps, as well as in other digital contexts, the *form* and *content* of users' consent is the main legal focus point, rather than the *communication* between the data subject and controller.[30] Moreover, in all the apps investigated there is a construction of an informed and autonomous user with presupposed agency to carefully read and understand the terms and conditions of the menstruapps,[31] even when such terms are described on an external website, rather than the app itself. This constructed independent, informed and technologically skilled user is, in addition, assumed to accept all the terms stated (or even unstated) in the menstruapp's privacy policies. In some cases, when disagreeing to specific terms, such as third-party personal data sharing, the data subject was expected to take extraordinary measures to revoke them, such as emailing the data controller. It is possible that the assumption about the well-equipped and well-informed 'techno global' user is modelled on the applications' developers. However, it is less likely to be equally appropriate for all the users of menstruapps, who use the apps in a range of different geographical, educational, social, ethnic, cultural, linguistic and economic settings. This inaccurate assumption creates a systemic disadvantage for data subjects, who are more disadvantaged the further from the techno global norm they are

[30] A similar conclusion has been made in the context of bioethics by Manson and O'Neill (2007).

[31] Hewer (2019, 288) makes a similar observation regarding informed consent in bioethics.

Table 2 Data subject's possibilities to revoke consent or to delete collected data

Menstruapp	Data subject can revoke their consent to future data collection	Collected data can be deleted if the user wishes
Clue (BioWink)	Yes	Yes
Period Tracker (Simple Design Ltd.)	Yes	Not mentioned in privacy policies, but in-app possibility
Flo: Period Tracker (Flo Health)	Yes	Yes
Period Tracker (Leap Fitness Group)	Yes	Not mentioned in privacy policies, but in-app possibility
Period Tracker (GP International LLC)	Yes	Yes
Period Calendar, Cycle Tracker (SimpleInnovation)	Yes	Yes
Period Tracker (Amila)	Yes	Yes

(for example, people who are unfamiliar with tech jargon or whose native language is not English). This, inevitably, creates an intersectional element of exploitation which can be depicted as digital period poverty.[32]

Compatibility with EU Legal Standards

Scrutinising the menstruapps in the light of EU data protection and particularly the GDPR, it should be highlighted that, in general, the practices relating to the validity of data subjects' consent, and particularly explicit consent, fail to fulfil even minimum requirements.[33]

Firstly, notwithstanding some exceptions (such as BioWink's Clue), it is often unclear what kind of personal data menstruapps process and potentially share with third parties according to their privacy policies. Moreover, possible third parties are seldom identified in specific terms. When factors such as the identity of third parties, the details on the purpose and use of personal data and the nature of the data processed remain unspecified and unreported, the consent given by data subjects to accept such vague terms cannot be considered granular. Accordingly, consent given under such conditions can hardly be considered *informed* or *specific* in line with the requirements for validity laid down in GDPR Art. 4(11).

Secondly, even though some of the apps investigated specifically asked for users' consent to personal data processing at the outset, it is also relatively common that such consent is assumed. Following the GDPR's requirements for valid, *unambiguous* consent and the earlier-mentioned CJEU's 'Planet49' doctrine, consent cannot be presumed. It cannot, for example, be obtained through pre-ticked consent boxes, but must be the result of the data subject's active choice. Hence, the menstruapps that did not ask for consent also fail to live up to EU data protection law in this regard.

Thirdly, a precondition for using many of the menstruapps was to agree to personal data processing and even third-party data sharing. Here, data subjects' wishes to share their personal data with the data controller, on the one hand, and third parties such as Google Analytics, on the other, cannot be collapsed.[34] Importantly, data subjects' consent in such a 'take-it-or-leave-it' scenario is not considered as *freely given* according to the GDPR.[35] Moreover, making consent for personal data sharing with third parties a precondition for using the app creates a difficult dilemma. As such, it forces the data subject to choose between not using the app at all, or alternatively, consenting to invasive personal data processing. The latter often involves data sharing with third parties, the sharing chain of which is practically impossible

[32] On this phenomenon, see Bloody Good Period and Women for Refugee Women (2019).

[33] It is possible that the privacy policies and/or the general practices of the menstruapps investigated not only fail to fulfil the data protection requirements laid down in GDPR art. 9, but also art 13, 15, 16 and 17. A legal evaluation of the compatibility with the GDPR as a whole is, nevertheless, beyond the scope of this article.

[34] Moreover, not informing data subjects about the identity of the controller and the recipients or categories of recipients of the personal data is illegal according to the GDPR art 13(1)(a) and (1)(e).

[35] art 7(4).

to trace. The EDPB guidelines on consent do not consider that consent in such cases is free:

> Article 7(4) GDPR indicates that, inter alia, the situation of 'bundling' consent with acceptance of terms or conditions, or 'tying' the provision of a contract or a service to a request for consent to process personal data that are not necessary for the performance of that contract or service, is considered highly undesirable. If consent is given in this situation, it is presumed to be not freely given (recital 43) (EDPB 2020, para 26).

Finally, as stated earlier, since the information processed by menstruapps concerns the sexual and reproductive health of their users, the consent requirements are higher. Accordingly, Article 9 of the GDPR requires that data subjects explicitly consent for such data processing to be allowed. For example, by sending an email, giving an oral statement or uploading her scanned signature, the individual has to expressly state that she consents to such sensitive and intimate data processing. Importantly, none of the menstruapps investigated require such actions on behalf of their users, which indicates that they fail to fulfil the legal requirements on sensitive data processing according to EU data protection law.

Reformulating Explicit Consent Through the Freedom to Negotiate

The former section showed that there are clear examples when menstruapps fail to live up to standards on consent as determined in EU data protection law. If the current legal standards, particularly those concerning explicit consent for sensitive data as special categories of personal data (GDPR Article 9), were enforced by data controllers, it might arguably increase data subjects' awareness, right to privacy and data protection. However, the failures to obtain explicit consent are also indicative of data controllers' general disregard of the data subject's desires. The lack of a normative difference between the contents of explicit versus regular consent in EU law de jure also, at least in the case of menstruapps, seems to lead to a de facto collapse of the categories. Such a disintegration of normative categories, in turn, inevitably leads to the weakening of the special protection of sensitive data regulated in GDPR Article 9. Hence, EU data protection law is in its conceptualisation of regular and explicit consent facilitating an evasive approach by data controllers (see also Koops 2014; Lynskey 2014; Daly 2016). To reimagine these concepts, the focus is now again turned to the freedom to negotiate (Palmer 2013, 2017).[36]

The validity standards of explicit consent concerning sensitive data in EU data protection law are unable to change the *terms* of the contract entered into by the data subject. As such, the standards concerning explicit and regular consent build on a situation where the app provider always already decides the terms of the agreement.

[36] For important, more comprehensive earlier contributions that reimagine data protection standards, see Cohen (2012), Nissenbaum (2009), Daly (2016).

Hence, the legal standards do not build on the communication between the data controller and the data subject (see Manson and O'Neill 2007).

In relation to menstruapps, the concept of freedom to negotiate provides a different point of view when analysing users' consent. Instead of analysing the form through which the user has or has not agreed, or the contents of the privacy policies, the concept scrutinises the (lack of) negotiating power possessed by data subjects. Do individuals have real power to determine or even affect the terms of the contract? In the example apps investigated in this paper, users have no influence over what the agreement between them and the app provider looks like. Data subjects have, for example, no possibilities of drafting alternative agreements if they do not agree to the terms dictated by the controller. Some, albeit limited, in-app options to agree to some terms and not others are given, which should be welcomed, as they give users increased abilities to affect the contract. Similarly, some of the app providers give users possibilities to email them when they wish to withdraw their consent, which also empowers data subjects to affect the terms of the contract. However, emailing can—in comparison to in-app options to tailor contract terms—be considered an alternative that requires more effort and technical and linguistic abilities on behalf of the data subject. It might, as such, also be less accessible to the individual users, using the app in a diversity of contexts.

Some reservations are nevertheless in place when thinking about data subjects' freedom to negotiate. Firstly, in a digital context, the communication between data subjects and controllers is, understandably, different and more limited in comparison to, for example, sexual encounters between natural persons, also affecting the freedom to negotiate. Secondly, app providers construct privacy policies that apply to the millions of data subjects downloading the apps. This raises a serious point of feasibility when it comes to users' abilities to negotiate individual agreements to suit their own needs and wishes. These two practical points are important reminders that there is a need for more innovative and transparent technological solutions for data subjects to customise their data processing choices. In-app options allowing individuals to agree to some kinds of data processing and not others and interactive, user-friendly software interfaces allowing easy communication with data controllers are examples of such solutions.

Such reservations notwithstanding, reimagining current standards in the light of the freedom to negotiate allows for more focus to be placed on the context, power imbalances and communication. Inspired by Palmer's model on sexual encounters (2013, 6), the differences in approach could be the following (Table 3):

Reimagining supranational normative standards in line with the freedom to negotiate could place more focus on data controllers, the possibilities of the data subject to negotiate the terms of the agreement, the power imbalance between the parties and the subjective experience of data subjects. In comparison to current standards on sensitive data, such a move allows for a different way of thinking about how a contract is drafted, rather than simply whether the user agrees

Table 3 Current conceptualisations of consent and freedom to negotiate

	Consent (GDPR)	Freedom to negotiate
Focus	Data subject ⇒ Has the data subject consented or not?	Data controller ⇒ Has the data controller restricted the data subject's freedom?
Relation	One-sided ⇒ Data controller proposes and data subject accepts or does not accept	Mutual, interactive process concerning what kind of relation to engage in and what the agreement will look like
Context	The moment when the data subject agrees or disagrees	The relationship and power imbalance between the data subject and the data controller
Choice	Does the data subject agree or not?	Does the data subject feel like she has a choice?

or not to already-drafted agreements. This could also allow for a more robust legal conceptualisation of data subjects' consent.

Towards a Feminist Ethics of Data

This article has theoretically, doctrinally and empirically shed light on the European legal standards pertaining to explicit consent and intimate data and investigated how they apply to menstruapps and how they are formulated in practice. It has shown how popular menstruapps—which turn menstruation into data that are quantified, researched and sold—in their conceptualisation of consent fail to live up to EU law. This article is an attempt to bring the topic of menstruapps into a critical legal discussion. It provides a feminist critique of the concept of consent prevalent in contemporary supranational EU law, particularly the notion of explicit consent in the GDPR. Advancing a normative, contextual and communicative model for rethinking the consent standards surrounding sensitive data, the findings of this article are pertinent to other forms of health-tracking applications.

There is, conclusively, a need to think critically about the commercial use of intimate data at all points of data processing, not merely when the data subject starts using an application and accepts its privacy policy. What happens after consent is given? How are the individual desires, needs and wishes of the data subject taken into consideration by data controllers? How can ethical data processing be enforced in practice? How can ethical data processing be balanced against monetisation of personal and intimate data? There is a need to critically interrogate, regulate and control the whole market of intimate data and to reform the institutional response to this market, promoting software apps that move away from exploitative business models.[37] As the lines between our physical and data bodies are blurred, intimate data processing needs normative standards and guidelines for its ethical use. The feminist freedom to negotiate provides a point of departure.

Acknowledgements This article is the result of research carried out by the author within the research project Intimacy in Data-driven Culture (grant number 327391), funded by the Strategic Research Council at the Academy of Finland. The author would like to thank Saara Monthan for her diligent research assistance. The author also particularly appreciates the extremely helpful comments by the anonymous reviewers and the editors of FLS, who all fostered the development of the article. Finally, special thanks to Jonna Genberg, Pia Eskelinen, Aleida Luján Pinelo, Johanna Niemi, Juho Aalto, Matilda Merenmies, Anne Alvesalo-Kuusi, Elina Pirjatanniemi, Juha Lavapuro and Magdalena Kmak for their valuable comments, encouragement and support for this paper.

Funding Open Access funding provided by University of Turku (UTU) including Turku University Central Hospital.

[37] An incentive to promote such a development could, apart from increased legal regulation, be public and institutional support of alternative period trackers that do not share personal data. An example is the menstruapp Drip by Bloody Health. The initiative receives German public funding.

References

Ahmed, Sara. 2017. No. f*eministkilljoys*, 30 June https://feministkilljoys.com/2017/06/30/no/. Accessed 9 June 2020.

Amila. 2019. Privacy Policy. *Amila,* 4 December. https://amila.io/apps/period/privacy.html. Accessed 3 Aug 2020.

Amnesty International. 2019. *Surveillance Giants: How the Business Model of Google and Facebook Threatens Human Rights*. London: Amnesty International Ltd.

App Store. 2020. Period Tracker—Eve. https://apps.apple.com/us/app/period-tracker-eve/id1002275138. Accessed 10 August 2020.

Anderson, Michelle J. 2004. Negotiating Sex. *Southern California Law Review* 78: 1401–1438.

Benoliel, Uri, and Samuel Becher. 2019. The Duty to Read the Unreadable. *Boston College Law Review* 60: 2255–2296.

Bloody Good Period and Women for Refugee Women. 2019. The Effects of "Period Poverty" Among Refugee and Asylum-Seeking Women. https://e13c0101-31be-4b7a-b23c-df71e9a4a7cb.filesusr.com/ugd/ae82b1_22dcc28fa137419abf5c9abe6bbf3b45.pdf. Accessed 14 July 2021.

Brosnan, Liz, and Eilionóir Flynn. 2017. Freedom to Negotiate: A Proposal Extracting 'Capacity' from 'Consent.' *International Journal of Law in Context* 13: 58–76.

Brownsword, Roger. 2004. The Cult of Consent: Fixation and Fallacy. *King's College Law Journal* 15: 223–251.

Clue. 2020. Clue Privacy Policy. https://helloclue.com/privacy. Accessed 3 August 2020.

Coding Rights. 2016. MENSTRUAPPS—How to Turn Your Period into Money (for Others). https://chupadados.codingrights.org/en/menstruapps-como-transformar-sua-menstruacao-em-dinheiro-para-os-outros/. Accessed 8 June 2020.

Cohen, Julie E. 2012. *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice*. New Haven: Yale University Press.

Cohen, Julie E. 2019. Turning Privacy Inside Out. *Theoretical Inquiries in Law* 20: 1–31.

Criado Perez, Caroline. 2019. *Invisible Women: Exposing Data Bias in a World Designed for Men*. New York: Vintage.

Daly, Angela. 2015. The Law and Ethics of "Self-quantified" Health Information: An Australian Perspective. *International Data Privacy Law* 5: 144–155.

Daly, Angela. 2016. *Private Power, Online Information Flows and EU Law: Mind the Gap*. Oxford: Hart.

Datenethikkommission. 2019. *Opinion of the Data Ethics Commission: Executive Summary*. Data Ethics Commission.

EDPB. 2020. *Guidelines 05/2020 on Consent Under Regulation 2016/679. Version 1.0.* Adopted on 4 May 2020.

Epstein, Daniel A., Nicole B. Lee, Jennifer H. Kang, Elena Agapie, Jessica Schroeder, Laura R. Pina, James Fogarty, Julie A. Kientz, and Sean A. Munson. 2017. Examining Menstrual Tracking to Inform the Design of Personal Informatics Tools. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (CHI 17) 6876–6888. New York: ACM Press.

Federici, Silvia. 2014. *Caliban and the Witch: Women, the Body and Primitive Accumulation*. New York: Autonomedia.

Flo Health. 2020. Privacy Policy. https://flo.health/privacy-policy. Accessed 3 August 2020.

Forbrukerrådet [The Norwegian Consumer Council]. 2020. *Out of Control: How Consumers are Exploited by the Online Advertising Industry*. Oslo: Forbrukerrådet.

Fox, Sarah, and Daniel A. Epstein. 2020. Monitoring Menses: Design-Based Investigations of Menstrual Tracking Applications. In *The Palgrave Handbook of Critical Menstruation Studies*, ed. Chris Bobel, et al., 733–750. London: Palgrave Macmillan.

Fraser, Nancy. 2013. *Fortunes of Feminism: From State-Managed Capitalism to Neoliberal Crisis*. London and New York: Verso.

Fultner, Barbara. 2013. Gender, Discourse and Non-essentialism. In *Dialogue, Politics and Gender*, ed. Jude Browne, 52–80. Cambridge: Cambridge University Press.

Gonzalez Fuster, Gloria. 2014. *The Emergence of Personal Data Protection as a Fundamental Right of the EU*. New York: Springer.

GP Apps. 2020. Privacy Policy. https://gpapps.com/support/privacy-policy/. Accessed 3 August 2020.

Hewer, Rebecca. 2019. Vulnerability and the Consenting Subject: Reimagining Informed Consent in Embryo Donation. *Feminist Legal Studies* 27: 287–310.

Information Commissioner's Office. 2020. What is Valid Consent? https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/what-is-valid-consent. Accessed 19 November 2020.

Jia, Lianrui, and Lotus Ruan. 2020. Going Global: Comparing Chinese Mobile Applications' Data and User Privacy Governance at Home and Abroad. *Internet Policy Review* 9: 1–22.

Kazan, Patricia. 1998. Sexual Assault and the Problem of Consent. In *Violence Against Women: Philosophical Perspectives*, ed. Stanley G. French, Wanda Teays, and Laura M. Purdy, 27–42. Ithaca, New York: Cornell University Press.

Koops, Bert-Jaap. 2014. The Trouble with European Data Protection Law. *International Data Privacy Law* 4: 250–261.

Kosta, Eleni. 2013. *Consent in European Data Protection Law*. Leiden: Brill.

Lahiri-Dutt, Kuntala. 2015. Medicalising Menstruation: A Feminist Critique of the Political Economy of Menstrual Hygiene Management in South Asia. *Gender, Place & Culture* 22: 1158–1176.

Leap. 2020. Privacy Policy. https://leap.app/privacypolicy.html. Accessed 3 August 2020.

Leibenger, Dominik, Frederik Möllers, Anna Petrlic, Ronald Petrlic, and Christoph Sorge. 2016. Privacy Challenges in the Quantified Self Movement—An EU Perspective. *Proceedings on Privacy Enhancing Technologies* 4: 315–334.

Li, Kathy, Iñigo Urteaga, Chris H. Wiggins, Anna Druet, Amanda Shea, Virginia J. Vitzthum, and Noémie Elhadad. 2020. Characterizing Physiological and Symptomatic Variation in Menstrual Cycles Using Self-tracked Mobile-Health Data. *NPJ Digital Medicine* 3: 79–92.

Lupton, Deborah. 2015. Quantified Sex: A Critical Analysis of Sexual and Reproductive Self-tracking Using Apps. *Culture, Health & Sexuality* 17: 440–453.

Lynskey, Orla. 2014. Deconstructing Data Protection: The 'Added-Value' of a Right to Data Protection in the EU Legal Order. *International & Comparative Law Quarterly* 63: 569–597.

MagicGirl. 2020. Teen Period Tracker. https://magicgirl.me/. Accessed 10 August 2020.

Manson, Neil C., and Onora O'Neill. 2007. *Rethinking Informed Consent in Bioethics*. Cambridge: Cambridge University Press.

Mantelero, Alessandro. 2014. The Future of Consumer Data Protection in the E.U. Re-thinking the "Notice and Consent" Paradigm in the New Era of Predictive Analytics. *Computer Law & Security Review* 30: 643–660.

MyFloTracker. 2020. Functional Medicine Period Tracker and Hormone Balancing App. https://myflotracker.com/. Accessed 10 August 2020.

NHS. 2021. NHS Gives Women Human Papillomavirus Virus (HPV) Home Testing Kits to Cut Cancer Deaths. https://www.england.nhs.uk/2021/02/nhs-gives-women-hpv-home-testing-kits-to-cut-cancer-deaths/. Accessed 22 July 2021.

Nissenbaum, Helen. 2009. *Privacy in Context: Technology, Policy and the Integrity of Social Life*. Stanford: Stanford University Press.

Nissenbaum, Helen. 2011. A Contextual Approach to Privacy Online. *Daedalus* 140: 32–48.

Office of the Data Protection Ombudsman. 2020. Consent of the Data Subject. https://tietosuoja.fi/en/consent-of-the-data-subject. Accessed 19 November 2020.

O'Loughlin, Kristen, Martha Neary, Elizabeth C. Adkins, and Stephen M. Schueller. 2019. Reviewing the Data Security and Privacy Policies of Mobile Apps for Depression. *Internet Interventions* 15: 110–115.

Palmer, Tanya. 2013. Sex and Sexual Violation in the Criminal Law: Findings from a Study into How People Distinguish Sex from Sexual Violation. *University of Bristol: ESRC,* June. https://tanya

vpalmer.files.wordpress.com/2013/04/sex-and-sexual-violation-in-the-criminal-law-june-2013.pdf. Accessed 22 July 2021.

Palmer, Tanya. 2017. Distinguishing Sex from Sexual Violation: Consent, Negotiation and Freedom to Negotiate. In *Consent: Domestic and Comparative Perspectives*, ed. Alan Reed et al., 9–24. Abingdon: Routledge.

Parker, Lisa, Tanya Karliychuk, Donna Gillies Gillies, Barbara Mintzes, Melissa Raven, and Quinn Grundy. 2017. A Health App Developer's Guide to Law and Policy: A Multi-sector Policy Analysis. *BMC Medical Informatics and Decision Making* 17: 1–13.

Pateman, Carol. 1980. Women and Consent. *Political Theory* 8: 149–168.

Peña, Paz, and Joana Varon. 2019. Consent to Our Data Bodies: Lessons from Feminist Theories to Enforce Data Protection. *Coding Rights*, 25 March. https://codingrights.org/docs/ConsentToOurDataBodies.pdf. Accessed 8 June 2020.

Privacy International. 2019. No Body's Business But Mine: How Menstruation Apps are Sharing Your Data. https://privacyinternational.org/long-read/3196/no-bodys-business-mine-how-menstruations-apps-are-sharing-your-data. Accessed 8 June 2020.

Rizk, Vanessa, and Dalia Othman. 2016. Quantifying Fertility and Reproduction Through Mobile Apps: A Critical Overview. *Arrow* 22: 13–21.

Rouvroy, Antoinette, and Yves Poullet. 2009. The Right to Informational Self-determination and the Value of Self-development: Reassessing the Importance of Privacy for Democracy. In *Reinventing Data Protection?*, ed. Serge Gutwirth, et al., 45–76. New York: Springer.

Schaper, Manuel, and Silke Schicktanz. 2018. Medicine, Market and Communication: Ethical Considerations in Regard to Persuasive Communication in Direct-to-Consumer Genetic Testing Services. *BMC Medical Ethics* 19: 1–11.

SimpleInnovation. 2019. Period Calendar, Cycle Tracker—Privacy Policy. http://privacy.simpleinnovation.us/simpleinnovation/period-calendar/privacy-policy-en.pdf. Accessed 3 August 2020.

Simple Design. 2020. Privacy Policy. http://simpledesign.ltd/privacypolicy.html. Accessed 3 August 2020.

Smart, Carol. 1989. *Feminism and the Power of Law*. London: Routledge.

Solove, Daniel J. 2013. Introduction: Privacy Self-management and the Consent Dilemma. *Harvard Law Review* 126: 1880–1903.

Sunyaev, Ali, Tobias Dehling, Patrick L. Taylor, and Kenneth D. Mandl. 2015. Availability and Quality of Mobile Health App Privacy Policies. *Journal of the American Medical Informatics Association* 22: 28–33.

UN Women. 2019. Infographic: End the Stigma. Period. https://www.unwomen.org/en/digital-library/multimedia/2019/10/infographic-periods. Accessed 10 August 2020.

Young, Iris Marion. 2005. *On Female Body Experience: "Throwing Like a Girl" and Other Essays*. Oxford: Oxford University Press.