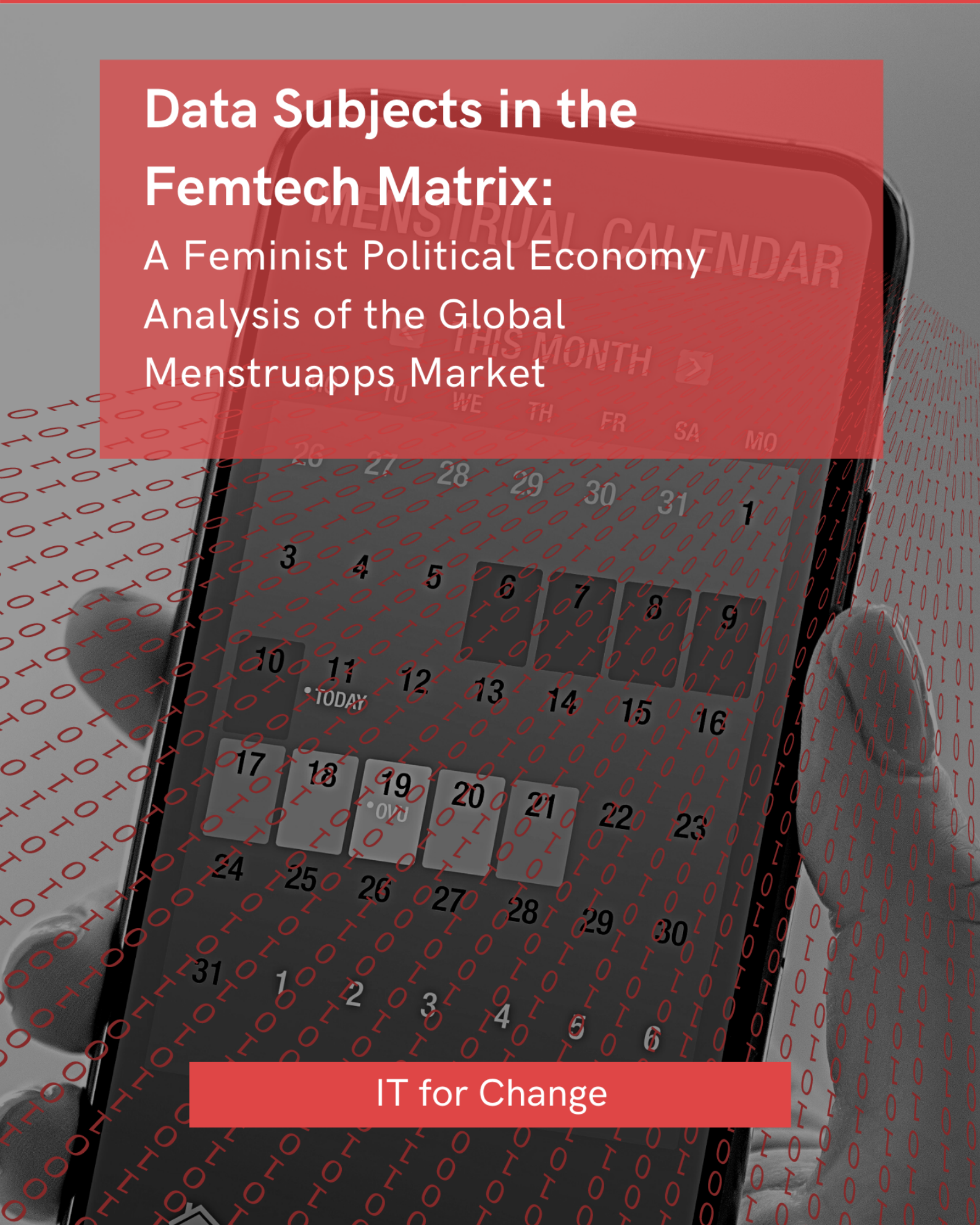
feminist digital justice

Issue Paper 6 | December 2021

Data Subjects in the Femtech Matrix:

A Feminist Political Economy Analysis of the Global Menstruapps Market



IT for Change

Feminist Digital Justice is a collaborative research and advocacy initiative of IT for Change and DAWN (Development Alternatives with Women for a New Era). We aim to reinterpret the emerging techno-social paradigm from a Southern feminist standpoint. The project foregrounds debates at the intersection of enduring feminist concerns about gender justice and women's human rights on the one hand, and emerging issues at the digital frontier on the other.

IT for Change is a Bengaluru based not-for-profit organisation engaged in research, policy advocacy and field practice at the intersections of digital technologies and social change, with a specific focus on social justice and gender equality.
See www.itforchange.net for more

Development Alternatives with Women for a New Era (DAWN) is a network of feminist scholars,researchers and activists from the economic South working for economic and gender justice and sustainable and democratic development.
See http://dawnnet.org/about/ for more.

This study was undertaken with support from the World Wide Web Foundation.

Conceptualization Anita Gurumurthy and Nandini Chami

Research Literature Review: Nandini Chami, R. Vaishno Bharati, Ankita Aggarwal
Key Informant Interviews: R. Vaishno Bharati, Ankita Aggarwal | Legal Review of Apps: Anushka Mittal, Nandini Chami

Lead author Nandini Chami | **Co-authors** R. Vaishno Bharati, Anushka Mittal, Ankita Aggarwal

Editorial guidance and review Anita Gurumurthy

Copy edit Sneha Bhagwat | **Design and layout** Sreemoyee Mukherjee

Cite as: Chami, N., Bharati, R. V., Mittal, A., & Aggarwal, A. (2021). Data Subjects in the Femtech Matrix: A Feminist Political Economy Analysis of the Global Menstruapps Market. IT for Change.

feminist digital justice

Data Subjects in the Femtech Matrix:

A Feminist Political Economy Analysis of the Global Menstruapps Market

December 2021

feminist digital justice

Table of Contents

feminist digital justice

Data Subjects in the Femtech Matrix: A Feminist Political Economy Analysis of the Global Menstruapps Market

Abstract

There is a growing body of scholarship on how the menstruapps marketplace reinforces hetero-patriarchal stereotypes. This study attempts to contribute to this growing body of research, focusing on the erosion of privacy and data autonomy in the menstrual apps (popularly known as 'menstruapps') market, using a feminist political economy lens. Through qualitative interviews with digital rights activists and open source technology developers, and a legal review of the privacy policies of four popular mobile applications (apps) in the Global South, this study explores two main questions:

(a) How do menstruapps in the femtech market address privacy (in collection, processing, and third-party sharing of personal data)?

(b) What do data practices of dominant menstruapps suggest about data sovereignty? What are the particular implications for users in the Global South?

Overview

The global femtech[1] market was valued at approximately $22 billion in 2020 and is estimated to reach a market size of over $60 billion by 2027 (Stewart 2021). Menstruapps, which are mobile applications that track a user's reproductive cycle, sex life, and menstrual health to provide algorithmically-derived insights about their body, constitute a major segment – over 50% – of this market (Zachariah 2021). In fact, as early as 2016, menstruapps were identified as the fourth most popular among adults and second most popular among adolescent girls in the 'health apps' category (Felizi and Varon 2016).

Digital cultures of the 'quantified self' – an increasing tendency to adopt digital tools for self-tracking and self-monitoring of one's everyday physical, mental, and emotional performance – have paved the way for a business model in menstruapps predicated on sensitive personal data collection and aggregation. This produces a contradiction that has repeatedly surfaced in feminist research on the subject. On the one hand, in a context where self-knowledge about one's body is often discounted and delegitimized by professional health systems, such apps can help menstruating persons recover a sense of control and personal autonomy over the management of their reproductive health (Khan 2019). But on the other hand, because menstruapps are integrated into digital capitalism[2] and its data extractivist logic, the expansion of choice that users experience "is empowerment [only] insofar as it produces options and feelings of ease—but within a burdensome context which it does not fundamentally challenge" (Ford, Togni, and Miller 2019).

[1] A term applied to a category of software, diagnostics, products, and other services that use technology to focus on women's health.

[2] We use this term to refer to the contemporary stage in capitalism wherein data and data-enabled intelligence are pivotal to capital accumulation. The paper uses digital capitalism and surveillance capitalism interchangeably.

Thus, quantification tools enable empowering self-management for users while allowing app owners to extract sensitive personal data for private profit (Mishra and Suresh 2021). Mainstream apps also tend to focus on the fertility management needs of women in the reproductive age group who constitute a major consumer base for the emerging femtech market (Olsen 2021). Therefore, the tech design of these apps presumes fertility management to be their sole aim. This stereotypes the user as cis-female, heterosexual, and monogamous, without factoring in user requirements and preferences of menstruating persons of alternative sexual orientation or from non-normative gender locations (Fox and Epstein 2020; Epstein et al. 2017).

Even as the menstruapps marketplace perpetuates patriarchal stereotypes about sexuality as inevitably linked to procreation, it also poses numerous threats to the privacy, autonomy, and personal sovereignty of users. A significant body of literature in this area has focused on user experiences of non-consensual data collection, and the harmful impacts of excessive and intrusive data profiling practices. Specifically, over-broad and vague privacy policies with insufficient attention to purpose limitation, personal data categories beyond obvious personal identifiers, and tokenistic consent procedures with limited clarity on data sharing with third parties, have been identified time and again in research studies (Shipp and Blasco 2020; Felizi and Varon 2016).

This study aims to contribute to this body of scholarship, looking at the erosion of privacy and data autonomy in the menstruapps market from a feminist political economy lens. It situates the locus of analysis on "the points in the circulation of capital where subjects are individuated or dividuated for the purposes of extracting profit" (Weinberg 2017). Individuation, here, refers to the construction of the consuming, desiring, producing, individual subject. And dividuation, following Gilles Deleuze (1992), refers to the processes whereby subjects are rendered "non-sovereign" (ibid) in control societies of coding, decoding, and recoding. Dividuation occurs when subjects are stripped down to the modular information that is used for transactions valuable to capitalist control (P2PF Wiki 2021).

Extending this analytical lens, the study examines privacy policies and practices of menstruapps (and the femtech market) asking 'whose' data is collected 'by whom' and 'for what', within the global circuits of surveillance capitalism. It explores the control of app/platform owners (largely from the Global North) over the data of app users (especially from the Global South) for furthering platform business models predicated on a hetero-normative, gender-conservative data subjectivity and the associated processing of data for profiling and targeting.

Research Questions and Methodology

Building on the expanding body of research, this study focused on addressing two main questions:

- How do menstruapps in the femtech market address privacy (in collection, processing, and third-party sharing of personal data)?

- What do data practices of dominant menstruapps suggest about data sovereignty? What are the particular implications for users in the Global South?

Towards this, the study adopted a qualitative research methodology using the following data collection methods:

Review of privacy policies and terms of service of popular menstruapps in the Global South

Based on preliminary inputs from feminist digital rights activists in Asia, Africa, and Latin America, and analysis of app downloads statistics as on 14 December 2020, we honed in on four mainstream menstruapps with a significant user base in the Global South.

Name of the menstruapp	App provider	Link to privacy policy (last accessed Dec 5, 2021)
Clue	BioWink GmbH, Germany	https://helloclue.com/privacy
Flo	Flo Health Inc, USA	https://flo.health/privacy-policy#storage-and-international-personal-data-transfers
MyFLO	Flo Living LLC, USA	https://www.floliving.com/legal/
Period Tracker (Period Calendar Ovulation Tracker)	Simple Design Ltd, British Virgin Islands, British Overseas Territory	https://simpledesign.ltd/privacy/my_calendar.html

The privacy policies of the selected apps were analyzed to map the levels of disclosure about data collection, processing, storage, third-party data sharing, and secondary use; and to infer the legal regimes of data governance bounding these apps' operations.

Key informant interviews with feminist digital rights activists and app developers

We conducted in-depth, qualitative interviews with nine feminist digital rights activists from different countries, between December 2020-February 2021, to gather gender perspectives on menstruapps and their implications for data governance. We also interviewed two FOSS developers from the Germany-based teams behind the alternative menstruapps, 'drip'[3] and 'Periodical'[4] to explore the contours of femtech business models centered on user data sovereignty. The interviews were approximately 60-minutes long. Verbatim transcripts were prepared and then coded using a grounded theory approach, to generate analytical insights. Appropriate consent procedures were adopted for all data collection and processing.

Research Findings

Finding 1. Popular menstruapps fail to protect data privacy, exposing users to profiling risks in downstream processing.

Menstruapps collect some of the most intimate pieces of information about our personal lives:

[3] https://bloodyhealth.gitlab.io/

[4] https://play.google.com/store/apps/details?id=de.arnowelzel.android.periodical&hl=en_IN&gl=US

reproductive health histories, sexual behavior and preferences, contraception use, food habits and lifestyle, medication use, and so on. Many of these pieces of personal information have been found to be completely unnecessary for the informational service of predicting the period cycle of an individual user (Marsh 2020). Evidently, app providers are collecting user data with an eye on downstream data markets for secondary uses of such data, including targeted advertising and market research, and not just for app operation or customization of services (Shipp and Blasco 2020).

Our research demonstrates that current privacy policies of popular menstruapps do not carry adequate safeguards to protect the personal data sovereignty of users, both in relation to their ability to control the extent of personal data sharing and the downstream processing of their data once it becomes part of aggregate, anonymized data sets. We also found that the narrow interpretation of the right to privacy as the right to anonymity, ends up leaving data subjects unprotected against profiling harms.

Blanket consent: A pact between lion and sheep

To begin with, privacy policies of menstruapps demand blanket consent from users for the collection of an extremely wide and unspecific array of data points, without any option for data subjects to engage in selective boundary setting for information sharing. For instance, Clue's privacy policy says: "when you use the Clue app or when you go on our website—some personal and non-personal data is collected, stored, and analyzed using internal and third-party tools." An examination of the privacy policies of Flo, MyFLO, and Period Tracker demonstrates that there is a generous sprinkling of over-broad legal phrasing: "When you sign up to use the app, we may collect personal data about you such as"; or for instance, "Information [collected] may include [categories like]", and so on.

As reflected by one key informant:

> In one of the Doctor Who episodes, they show an alien race collecting energy from people through their TV sets, literally sucking energy out of their face. Sometimes, I feel like that when I use apps which ask for a lot of information, and menstruapps are very much a part of that. They take a lot of information with my knowledge, which I am supposedly consenting to […] Menstruapps need to have a very straight, actual reasoning for [the personal] information they are asking. I think that's how we can start setting boundaries for quantification. If you ask me to input data of the start and end date of my period, I can see why you would ask that. But if you're asking me for [information on] my sex drive, on what sort of pain I am feeling, my moods, what I am feeling, I need to know why are you asking me this. And how is this related to my menstrual health [needs].
>
> Key informant, name withheld

Such data practices are clearly against the spirit of informed consent enshrined in the personal data protection framework of the EU's General Data Protection Regulation (GDPR), which obliges data controllers[5] to provide data subjects with clear information regarding the purposes and legal basis under which their personal data will be processed, including third-party data sharing arrangements, right at the point of collection (Privacy International 2020a).

As another informant observed:

> This 'consent' is once and for all and you've to give it before entering the app. The pact between the menstruapp owner and you as the user is like a contract between a lion and a sheep!
>
> hvale vale, Association for Progressive Communications

Indiscriminate third-party data sharing: A take-it-or-leave-it predicament

Not only do popular menstruapps collect extensive personal information from data subjects without a baseline of prior and informed consent, they also share the aggregate datasets they hold with third parties, leaving users with no recourse except a total opt out from the app. MyFLO's privacy policy explicitly mentions that personal information, including sensitive health information, may be shared with its "third-party database", "third-party server for transferring information to [the app's] data dashboard", "third-party CRM for triggering email campaigns", and "data analytics services". The user is also not offered the choice to manage the boundaries of such sharing. The policy states bluntly that "If you are not comfortable with these information practices, your only recourse is not to use our site, app or service, in any way".

Apps also seem to take the view that the scrubbing of personal identifiers from user data through de-identification and/or anonymization in such data sharing arrangements is the only duty they owe users in third-party data sharing arrangements. Flo's privacy policy states: "We may aggregate, anonymize or de-identify your Personal Data so that it cannot reasonably be used to identify you. Such data is no longer Personal Data. We may share such data with our partners or research institutions." Flo's announcements of such collaborations in the public domain reveal that "partners" have included the bio-pharmaceutical company, Myovant Sciences (Flo Health Insights 2020a), and the pharmaceutical and life sciences company, Bayer AG (Flo Health Insights 2020b). What emerges is that once their data is part of an anonymized, aggregate pool, users simply lose control over its combining and recombining in secondary uses – a testimony to the ever-proliferating, yet, unregulated data markets in which big players have a huge stake.

[5]Article 4(7) of the General Data Protection Regulation (GDPR) defines a data controller as: the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

As the US Federal Trade Commission's much-publicized complaint against the Flo app demonstrates (Schiffer 2021), menstruapps blatantly violate even the narrow promise of the right to anonymity they make to users in their terms of service, freely sharing personal information, including sensitive information, with third-party advertisers. Even in jurisdictions where there is a high level of legal protection for individual privacy and personal data protection, such as the European Union, menstruapps have failed to uphold all legally guaranteed rights of their data subjects. A 2020 study of the privacy practices of 30 popular Android menstruapps found that none of the apps studied "were able to provide the necessary information on all privacy rights, as determined by GDPR", specifically in relation to user rights to data access, deletion, and portability (Shipp and Blasco 2020).

As our key informant, Chenai Chair, highlighted, such ambiguity around third-party data sharing leaves users with practically no way to extract accountability from the apps for the many purposes for which their data is utilized:

> Accountability is cross-cutting, in that you want to be able to see what's going on with my information; what are you doing with it…We should get updates from menstruapps on how they have worked with our data. I'm actually wondering, where's [sic] the transparency reports from menstruapps?…because they're collecting so much sensitive data.
>
> Chenai Chair, Mozilla Foundation

The Clue app is somewhat of an outlier in this scenario. Privacy International's (2020b) audit of menstruapps found that the list of third parties with which Clue shares data was listed in its privacy policy, as claimed by the app. In addition, Clue also seems to hold an ethical line with respect to third-party data sharing; its privacy policy states that the app shares de-identified personal data with "carefully vetted researchers to advance female health studies", and provides users a contact email ID, in case they want an opt-out option from their data being included in such research.

Notably, the collaborators seem to be almost exclusively from the US and EU. More importantly, there is no transparency about the criteria on which such collaborators are selected. This presents an accountability deficit of a different kind, about case-by-case opt-in options for users to share their data for specific instances of research, even if it is for the ostensible public good of scientific progress, as informant, Ambika Tandon, reflected:

> There needs to be clarity [for users] around what kind of research is going to be done on their data. Who are going to be the stakeholders? For example, if I were to think about how this would work in practice, I would maybe like to see a notification or some kind of question that the app would ask me? For example, are you comfortable with your data being [part of a dataset] shared with Institution X for research on this particular topic? And then I have a sort of sense of who are the parties who are going to be involved; what are the objectives; what is going to be the outcome?
>
> Ambika Tandon, Centre for Internet and Society

Profiling harms: Apps don't care

There is increasing recognition that the business model of menstruapps is predicated on profiling for advertising, and that information services – mostly inaccurate and unreliable advisories (Earle et al. 2020; Moglia 2016) – are just a hook. As informant, Arno Welzel, observed:

> When some company says, 'we do this for research purposes, and universities can use the data to do some research', I am not sure if this claim is really honest. I think [menstruapps] may do research on the data they collect. But I think the goal [of such research] is to sell more products. And this, I think is the real motivation. They want to understand how they can tailor products for women in a better way and in the end make more money off it, of course.
>
> Arno Welzel, technology developer (Periodical)

Period tracking certainly provides companies a gold mine of intimate information to profile and segment consumers. This is almost akin to a form of biopower, as informant, Marie Kochsiek, theorized:

> Apps do not care about me personally. [They] want to know that they can persuade users to buy some product and use data as a collective set. Do we want a [menstruapp] company to know the fertility rate of a city for the next year? This is definitely population politics.
>
> Marie Kochsiek, technology developer (drip)

As Sharlene Gandhi (2020) observes, in markets like the US, where menstruapps are not subject to laws governing health information processing, a "Black Mirror-esque fear arises when or if [period app] data is then inputted into tools like Facebook Audience Insights[6], a platform that openly targets ads using data points such as relationship status". This is not merely a theoretical/hypothetical scenario. Media reports already suggest that the pregnancy app Ovia seems to have become "a powerful monitoring tool for employers and health insurers, which under the banner of corporate wellness have aggressively pushed to gather more data about their workers' lives than ever before" (Harwell 2019).

But would the problem of profiling be solved through a data protection legislation? Scholarship on digital rights is telling us that the answer is no. The propertarian model of individual control over one's personal data is enshrined in the EU GDPR, being emulated by governments across the world, is increasingly being recognized as ineffectual in addressing the data-driven harms of group profiling that underpin most data business models today (Tisné and Schaake 2018).

This is because even if an individual data subject opts out of data sharing, and also exits a period app, they can still be subject to group profiling. As a recent analysis (Bourreau et al. 2020) of the profiling risks of the Google-Fitbit data deal eloquently highlights:

> Given Google's track record, predictions need not rely on individual/personal data: due to privacy externalities, it is enough for Google to correlate aggregate health outcomes with non-health outcomes for even a subset of Fitbit users that did not opt out from some use of using their data, to then predict health outcomes (and thus ad targeting possibilities) for all non-Fitbit users (billions of them).

This is why we need new frameworks to address harm mitigation in complex forms of downstream data use, especially in relation to the instances where individual controls over data are not sufficient protection (McMahon, Buyx, and Prainsack 2019).

Finding 2. Data flows from (users of the) South to (corporations of the) North puts users of femtech in the South at disproportionate risk of human rights violations.

Datafication processes have created a new form of social relations – data relations – that pave the way for a creeping capitalization of sociality that further entrenches global inequalities (Couldry and Mejias 2018). As feminist writing on digital capitalism also highlights, datafication amounts to an ever-expanding encroachment of "the intimate lifeworld" (Gurumurthy and Chami 2020).

Femtech's informatics of domination: reducing gender to pinks and roses

Popular menstruapps are part of this global circuit of digital capitalism which relies on a new imperial force, the 'Silicon Valley' business model of Big Tech, extracting data resources from the Global South

6 https://m.facebook.com/business/news/audience-insights

(Kwet 2019). As our key informant, Ingrid Brudvig, noted:

> These apps are a perverse translation of women's bodies into a system of production, so-called production, which is inherently extractive. The way that women's bodies are literally being used to feed [value creation for] the digital economy is really worrying.
>
> Ingrid Brudvig, Women at the Table

Just as the peoples of the Global South were divested of their territories and resources and became second-class citizens of capitalist modernity, surveillance capitalism also inscribes a new regime of coloniality; an 'informatics of domination" (Haraway 1985) in which only those ways of being, thinking, and feeling that serve the project of "modification, prediction, monetization, and control" of human behavior are permitted, and alternative worlds diminished (Zuboff 2019).

Informant, Catherine D'Ignazio, observed how femtech reinforces and promotes patriarchal, hetero-normative worldviews rooted in racist and colonial values:

> Data extractivism perpetuates geographical inequalities and colonial inequalities. So many of these [menstruapps] are designed in Silicon Valley, and [this is reflected in the] cultural constructions [of race and gender that] is presented in the apps. Often, it doesn't even work for the people from the US, [such as] the non-binary folks. It is sometimes offensive, like pink and roses. But I think those kind of biases and assumptions that are baked into these apps have [even more] problematic consequences when exported out to all the different locations of the world because they simply don't match the way in which people think of themselves or think of themselves in the relation to their families, societies and cultures, etc. And then the risk, the same risk like in the US, is like that of imperialism, that people might feel normed into the US centered construction of gender.
>
> Catherine D'Ignazio, Data + Feminism Lab, MIT

In addition to the perpetuation of stereotypical, discriminatory, and exclusionary visions of gender, sexuality and race that have been well-documented in auto-ethnographic explorations of menstruapps, our research found how the political economy of digital capitalism opens up a minefield of concerns with respect to human rights violations and also places users from the Global South at additional risk.

Menstruapps and human rights: It's not all about privacy

Interviewees highlighted how critical perspectives on menstruapps cannot stop with privacy and personal data protection, but need to move into other foundational human rights, particularly sexual and reproductive rights. As Chenai Chair observed:

> Oftentimes, when advocacy [in the data governance space] happens, it just explores [intersections with] privacy, freedom of expression and access to information. But there isn't that spill over conversation of what does [a certain data practice] mean, in terms of other rights; your economic rights [in relation to] your sexual and reproductive health.
>
> Chenai Chair, Mozilla Foundation

Menstruapps may carry a disclaimer for the information they provide. For instance, Flo and Clue include prominent disclaimers that their PCOS assessments should not be construed as diagnoses (Singer 2019). But what gets missed out in the conversation about surveillance capitalism is how to fix corporate accountability for bodily harms stemming from the use of misleading health advisories.

As informant Jelen Paclarin observed:

> If you are from Southeast Asia, and a poor woman who had a miscarriage because you followed the app's advice, as you thought the app was telling the truth, what happens?
>
> Jelen C. Paclarin, Women's Legal and Human Rights Bureau

As the UN Economic and Social Council's (2016) General Comment No. 22 on the right to sexual and reproductive health observes, "All individuals and groups, including adolescents and youth, have the right to evidence-based information on all aspects of sexual and reproductive health, including, maternal health, contraceptives, family planning, sexually transmitted infections, HIV prevention, safe abortion and post-abortion care, infertility and fertility options, and reproductive cancer." When such information access is trapped within the platformized enclosures of digital capitalism, subjects who are otherwise under-served and marginalized become highly vulnerable to misinformation and its harmful consequences, without any recourse to redressal.

Data sovereignty: A neo-colonial fiction

In the liberal rhetoric on data rights, countries of the Global South are often criticized for weaponizing laws against their people; using data laws to sustain their authoritarian power over people (Arora 2019). This narrative of the culpability of illiberal governments – true as it may be – tends to hide the limitations of data rights regimes in the Global North; the inefficacy of the EU GDPR in tackling data-driven harms of group profiling being a case in point. It also masks another equally important reality – the uneven geographies of the data economy. Southern states often find themselves powerless in holding transnational digital corporations, operating virtualized businesses on their territories, accountable. As Jelen Paclarin observed, jurisdictional sovereignty has direct implications for access to justice:

> We always say state obligations, but then again, how about the obligations of corporations? If they have eventually been seen as contributing to discrimination or violation of privacy or consent related mechanisms, how do you file cases against them? When you invoke obligation of corporations, it is expensive; the app will say okay, but [file the dispute] in the US or in the EU court. How will I do that? Who will do that for me? Who will file this case? [My] government?
>
> Jelen C. Paclarin, Women's Legal and Human Rights Bureau

A similar set of issues crops up in third-party data sharing deals made by Northern digital companies with local apps. For example, Facebook struck a deal with the Indian app, Maya (Mandavia 2019) to access sensitive personal information of Maya's users. How would Indian users hold Facebook to account for cascading rights violations in future downstream uses of their data?

The EU GDPR protects data subjects only in its territorial jurisdiction. Citizens of countries outside Europe opting in for EU-based apps, therefore, cannot expect that their personal data would be protected by the same standards. As key informant, Sofia Scasserra, highlighted:

> Of course, Europe has a better data protection law, and that makes you think that a [menstruapp] from Europe may be better than an app from America. But, in the end, but it's all the same. Maybe [when operating] in Europe, they [app owners] won't be able to use [personal] information as widely they want to, but [elsewhere it is] data colonialism, and data extractivism, and […] doing exactly what Spain did to Latin America many centuries ago.
>
> Sofia Scasserra, Transnational Institute

Similarly, informant, Tara Patricia Cookson, highlighted how there were parallels between the extraterritorial rights violations of industrial corporations and the data rights violations of Northern digital companies in territories of the Global South:

> I would be interested in the connections or correlations that can be drawn with other products and services that are consumed through global trade and global commerce […] You can look at Canadian mining companies that go down to Peru and mine. There are different standards that they comply with than what they do in Canada.
>
> Tara Patricia Cookson, Ladysmith Collective

Ethics dumping in the data age – the export of unethical data analytics practices by digital companies to low- and middle-income countries with lower levels of data protection and less robust regulation – often aligns "with the old fault lines of colonialism" (Mohamed et al. 2020).

The data rights of women and other menstruating data subjects, including the right not to be subject to data processing without a legal basis (for example, informed consent), is indeed a function of domestic law and the de jure sovereignty of personhood that is vested in them through a bundle of guarantees. Yet, these rights may not be actionable at all given transnational corporations' de facto control over the data economy. The race for progress in the digital economy often means that countries in the Global South without data capabilities have no choice but to allow their (citizens') data to flow. Even if there were to be a domestic legal regime for personal data protection, the residual control rights that data subjects have is rendered non-actionable in a digital economy that is unequal and unjust. Affecting vulnerable populations disproportionately, this predicament harks back to the unholy marriage between the liberal international constitutionalism human rights regime and colonialism under corporate globalization. Under this regime, the very institutions and frameworks of international law become inextricably linked to the colonial project (Schwöbel-Patel 2017; Shetty 2018).

What emerges in our analysis is the need to situate gender politics in the menstruapps debate in relation to the axis of race and geography; particularly, the geo-economic and geo-political contours of digital capitalism in the current moment.

Conclusions

This study attempted to examine the implications of the global menstruapps market for the privacy and data sovereignty of app users, particularly those located in the Global South. Our analysis, deploying a feminist political economy lens, reveals how surveillance capitalism assimilates gendered bodies into its workings. A predatory market in femtech seeks huge payoffs through easy access to (data about) menstruating bodies. Menstruapps pursue new markets and feed Big Pharma with valuable resources, at the high moral cost of invading the intimate and eroding human rights. Holding up the tantalizing promise of personalized information to support users' period tracking and self-care, menstruapps pathologize natural, bodily processes, transfiguring menstruation into a desired object of surveillance capitalism.

Privacy policies and practices of popular menstruapps tend to be vague and ineffectual. Representing a scenario of no-holds barred data extractivism, their over-broad consent clauses lack not only purpose limitations of data use, but also procedural guarantees for the data subject's rights to access, deletion and portability. Despite the direct risk for users of undesirable outcomes arising from inappropriate advisories, for instance, unplanned pregnancies (Hunt 2020), the fine print of their terms of service reveals that popular menstruapps avoid any and all liability. Thus, users are left with no recourse for violations of their sexual and reproductive health and rights.

Further, users in the Global South face a double whammy in the lack of accountability of menstruapp owners for such violations. Oftentimes, their governments have not enacted legislation that protects them from the harmful impacts of behavioral data profiling by transnational digital corporations. Even if laws for personal data protection do exist, the de facto flows of data away from the countries of the South into enclosures of Northern corporations undermine the justiciability of user rights in the event of any abuse. The lack of a global governance regime that recognizes the jurisdictional sovereignty of nations and peoples over their data resources means that data subjects from the South forfeit residual control rights over the unknowable, future, non-consensual uses their data may be put to.

What we can conclude is a de-recognition of human rights and evisceration of ethics in platform models for intimate data about menstruating bodies, particularly from the Global South. As post-humanist scholarship has demonstrated (Hayles 1999, cited in Käll 2017), the dematerialization of the menstruating body for the apparatus of capitalist datafication implies not just a change in the material substrata (of physical bodies becoming data bodies) but also a change in the codes of representation (the cultural construction of assigning gender codes to bodies). In fact, data is economically valuable precisely because, in its aggregate, anonymized form, it represents abstracted knowledge about the social codes that manifest in, and through, behavioral sociality. Thus, it would be a grave error to

assume that once stripped of personal identifiers and aggregated, data becomes, and can be governed as, a purely economic resource. On the contrary, data is always social and our embodied identities are always entangled and implicated in its collection, aggregation, and processing. Therefore, data sovereignty is not only about the individual rights of data subjects to exercise full control over the collection, sharing, and all potential uses of their personal data. It is equally about ensuring that the social body-politic of data representing our bodies, life worlds, and socialities is not instrumentalized for the extractivist logic of data capital accumulation (Gurumurthy and Chami, forthcoming).

This connection to social power in the digital economy and the flows of data in the circuits of digital capitalism are crucial for a feminist approach to data ethics and governance. Proceeding from this starting point, we now reflect on some strategic directions to recover personal sovereignty from the femtech data matrix that need further theoretical and policy work.

First, a feminist approach to data sovereignty requires a democratically deliberated social norm about the very boundaries of data alienability to prevent surveillance capitalism from encroaching on our bodily autonomy. In the specific case of menstruapps, business models that profile sensitive and intimate information about sexuality and reproductive health for downstream market research should not be permitted to function. This will automatically ensure that menstruapps limit their data collection to the information that is essential to providing customized informational advisories, steering clear of unbounded personal information gathering. Equally importantly, sectoral legislation must be introduced for the femtech domain to ensure that menstruapp providers are held accountable for their data collection and third-party data sharing practices and for the accuracy of the information advisories they provide. They must be held to the same standards for protection of client confidentiality and safety, that any traditional health information service provision operating in the market may be held to.

Second, we need a new data governance regime that not only upholds the individual controls of all data subjects over their personal data, but also deals with the more complex challenge of leveraging data as a social knowledge commons for public value and benefit, so that people's claim to datafied intelligence is not mediated by market-based frameworks. In the case of menstruapps, and more broadly, femtech, this requires us to answer the question of how the social resource of aggregate, anonymized data about sexual and reproductive health needs and behavior can be deployed to enable the community of users, and indeed, non-users, to gain collective value and shared insight, with the guarantee of privacy, dignity and autonomy for all.

To do this, we need to recognize and ensure that unmet sexual and reproductive health information needs, especially of the most vulnerable communities in the Global South, are not just treated as a data business model waiting to be tapped. As internet and smartphone diffusion increases, ethically-designed and rights-enhancing femtech apps could fulfill informational needs (such as in menstrual health and hygiene) that may otherwise be unmet because of cultural stigmas/taboos. For example, UNICEF's Oky app provides age- and context-appropriate menstrual health advisories to young girls, also enabling them to track their period cycles. The app also ensures that all data entered by users is locally-

stored on their devices so that they have full control over who they want this data to be shared with, and on what terms (Tyers 2021).

Another equally important move would be to provide public support for designing and developing alternative femtech that is not extractive. Periodical, initiated as a community project with no external funding, and drip, developed with funding from Germany's Ministry of Education, are two good examples of alternative menstruapps that keep user data private by storing it only on the user's device. Support for initiatives could also extend – in the form of new legal-institutional mechanisms – to communities of interested individuals who wish to voluntarily pool their data for public interest science. This would lead to the flourishing of a feminist data collectivism that enables the commonsification of health (and other) data through the socialization of its value.

States have an obligation to deliver high quality health services, including information services, to women and gender minorities, as upheld by the Cairo Declaration on Population and Development (United Nations Population Fund 1994). The democratization of access and the datafication of public health systems presents an opportunity not only to disseminate health information on scale, but also to personalize health care through information pull functionalities. Hence, state-led data infrastructures – backed by appropriate laws and adequate implementation mechanisms – must be geared towards providing contextualized, gender-inclusive, evidence-based information. It is vital that data rights in such an infrastructure are not an afterthought, but intrinsic to their very design (Radhakrishnan 2021). Citizen participation, for co-designing and auditing these infrastructures from a human rights and gender justice perspective, is also non-negotiable in such public initiatives.

Third, a new global constitutionalism is needed for the governance of data, grounded in an indivisible, integrated vision of data rights that recognizes people's sovereignty over their data resources as integral to their personal autonomy, along with their right to development. The United Nations Conference on Trade and Development's (UNCTAD's) Digital Economy Report (2021) highlights the need for such an international governance framework that can enable gains from data flows to be equitably distributed within and between countries.

The prevailing intellectual property (IP) rights regime, especially in relation to Artificial Intelligence (AI) technologies, consolidates the enclosure of data and data-based intelligence by a few powerful corporations from advanced AI economies. This prevents alternative imaginaries of platform collectives and collaboratives from gaining ground. A foundational transformation of the IP regime is crucial for mainstreaming feminist visions of platform cultures.

The World Health Organization's (WHO's) Health Data Governance Summit, 2021 emphasized the need to secure health data as a global public good, with a data governance framework that can support and strengthen "both individuals and communities to have control over, and benefit from, their own health data" (WHO 2021). Given the vexatious history of digital corporations co-opting data public goods for their extractivist business models (and making women in the Global South easy targets, as

this study has shown), it is clear that any such governance framework can promote public benefit only if it includes clear safeguards. Compulsory licensing clauses may be one way forward to preserve the inappropriability of the knowledge generated through such data public goods.

Finally, the data matrix of menstruapps forces feminist activists to confront the deceptive rainbow hues of surveillance capitalism, readily accommodating diversity to instrumentalize people. The impact of digital corporations on women and gender minorities and their lifeworlds is no different from the violence and criminality unleashed by extractive mining industries on Black, indigenous, and other marginalized communities in the South. Therefore, mounting a struggle against the criminality and impunity of the digital behemoths is cardinal for the feminist agenda at the current conjuncture.

Endnotes

Arora, P. (2019). General Data Protection Regulation—A Global Standard? Privacy Futures, Digital Activism, and Surveillance Cultures in the Global South. Surveillance & Society, 17(5), 717-725.

Bourreau, M., Caffarra, C., Chen, Z., Choe, C., Crawford, G., Duso, T., Genakos, C., Heidhues, P., Peitz, M., Rønde, T., Schnitzer, M., Schutz, N., Sovinsky, M., Spagnolo, G., Toivanen, O., Valletti, T., & Vergé, T. (2020). Google/Fitbit will monetise health data and harm consumers. Retrieved December 1, 2021, from https://voxeu.org/article/googlefitbit-will-monetise-health-data-and-harm-consumers

Couldry, N. & Mejias, U. A. (2018). Data colonialism: Rethinking Big Data's relation to the contemporary subject. Television & New Media, 20(4), 336-349. doi:10.1177/1527476418796632

Deleuze, G. (1992). Postscript on the Societies of Control. October, 59, 3–7. http://www.jstor.org/stable/778828

Earle, S., Marston, H.R., Hadley, R., Banks, D. (2020). Use of menstruation and fertility app trackers: A scoping review of the evidence. BMJ Sexual & Reproductive Health 2021, 47(2), pp. 90-101. doi: 10.1136/bmjsrh-2019-200488

Epstein, D. A., Lee, N. B., Kang, J. H., Agapie, E., Schroeder, J., Pina, L. R., Fogarty, J., Kientz, J. A., & Munson, S. (2017). Examining menstrual tracking to inform the design of personal informatics tools. Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems. CHI '17: CHI Conference on Human Factors in Computing Systems. https://doi.org/10.1145/3025453.3025635

Felizi, N., & Varon, J. (2016). MENSTRUAPPS- How to turn your period into money (for others). Retrieved July 07, 2021, from https://chupadados.codingrights.org/en/menstruapps-como-transformar-sua-menstruacao-em-dinheiro-para-os-outros/

Flo Health Insights (2020a). Myovant Sciences and Flo Health partner to develop digital tool to screen women for heavy menstrual bleeding. (2020). Retrieved June 22, 2021, from https://flo.health/collaborations/innovations/myovant-sciences-and-flo-will-develop-tool-to-screen-heavy-menstrual-bleeding

Flo Health Insights (2020b). Flo Health, Bayer AG and Help Group Research Collaboration partner to raise awareness about heavy menstrual bleeding. (2020). Retrieved June 22, 2021, from https://flo.health/collaborations/innovations/flo-health-and-bayer-help-group-research-collaboration

Ford, A., De Togni, G., & Miller, L. (2021). Hormonal health: Period tracking apps, wellness, and self-management in the era of surveillance capitalism. Engaging Science, Technology, and Society, 7(1), 48-66.

Fox, S. & Epstein, D. A. (2020). Monitoring menses: Design-based investigations of menstrual tracking applications. In C. Bobel, I. T. Winkler, B. Fahs, K. A. Hasson, E. A. Kissling, & T.-A. Roberts, The Palgrave Handbook of Critical Menstruation Studies (pp. 733-750). Palgrave Macmillan.

Gandhi, S. (2019). Are your period tracker apps exploiting your sensitive personal data?. Retrieved December 1, 2021, from https://gal-dem.com/are-your-period-tracker-apps-exploiting-your-sensitive-personal-data/

Gurumurthy, A. & Chami, N. (2020). The deal we always wanted: A feminist action framework for the digital economy. FES. Retrieved Dec 07, 2021 from https://www.fes.de/en/themenportal-gender-jugend/gender/the-future-is-feminist/the-deal-we-always-wanted

Gurumurthy, A. & Chami, N. (forthcoming) Beyond data bodies: New directions for a feminist theory of data sovereignty. Data Governance Network.

Haraway, D. (1985). A cyborg manifesto. The Anarchist Library. Retrieved December 07, 2021, from https://theanarchistlibrary.org/library/donna-haraway-a-cyborg-manifesto

Harwell, D. (2019). Is your pregnancy app sharing your intimate data with your boss?. Washington Post. Retrived December 06, 2021, from https://www.washingtonpost.com/technology/2019/04/10/tracking-your-pregnancy-an-app-may-be-more-public-than-you-think/

Hunt, K. (2020). Fertility apps can be 'misleading' for women, review finds. CNN. Retrieved December 06, 2021, from https://

edition.cnn.com/2020/04/06/health/fertility-period-contraceptive-apps-trackers-wellness/index.html

Käll, J. (2017). A posthuman data subject? The right to be forgotten and beyond. German Law Journal, 18(5), 1145-1162.

Khan, S. (2019, June 07). Data bleeding everywhere: A story of period trackers. Retrieved July 04, 2021, from https://deepdives.in/data-bleeding-everywhere-a-story-of-period-trackers-8766dc6a1e00

Kwet, M. (2019, March 13). Digital colonialism is threatening the Global South. Retrieved from https://www.aljazeera.com/opinions/2019/3/13/digital-colonialism-is-threatening-the-global-south

Mandavia, M. (2019). Period-tracking app Maya shares users personal data with Facebook. Economic Times. Retrieved December, 06, 2021 from https://economictimes.indiatimes.com/tech/internet/period-tracking-app-maya-shares-users-personal-data-with-facebook/articleshow/71067864.cms

Marsh, S. (2020). Menstruation apps store excessive information, privacy charity says. Retrieved December 01, 2021, from https://www.theguardian.com/society/2020/dec/21/menstruation-apps-store-excessive-information-privacy-charity-says

McMahon, A., Buyx, A., & Prainsack, B. (2019). Big Data governance needs more collective responsibility: The role of harm mitigation in the governance of data use in medicine and beyond. Medical Law Review, 28(1), winter, 155-182. doi: https://doi.org/10.1093/medlaw/fwz016

Mishra, P., & Suresh, Y. (2021). Datafied body projects in India: Femtech and the rise of reproductive surveillance in the digital era. Asian Journal of Women's Studies, 1-10. doi:10.1080/12259276.2021.2002010

Mohamed, S., Png, M., & Isaac, W. (2020). Decolonial AI: Decolonial theory as sociotechnical foresight in artificial intelligence. Philosophy & Technology, 33(4), 659-684. doi:10.1007/s13347-020-00405-8

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), pp. 1153-1160. doi: 10.1097/AOG.0000000000001444

Olsen, E. (2021). Why femtech needs to move past reproductive healthcare. Retrieved December 01, 2021, from https://www.mobihealthnews.com/news/why-femtech-needs-move-past-reproductive-healthcare

P2PF Wiki. Dividuation. Accessed 2021. https://wiki.p2pfoundation.net/Dividuation

Privacy International. (2020a). No body's business but mine: How menstruation apps are sharing your data. Retrieved October 13, 2020, from https://www.privacyinternational.org/long-read/3196/no-bodys-business-mine-how-menstruations-apps-are-sharing-your-data

Privacy International. (2020b). We asked five menstruation apps for our data and here is what we found.... Retrieved July 20, 2021, from https://privacyinternational.org/long-read/4316/we-asked-five-menstruation-apps-our-data-and-here-what-we-found

Radhakrishnan, R. (2021). Your health data is others' wealth. Retrieved December 06, 2021, from https://in.boell.org/en/2021/11/02/your-health-data-others-wealth

Schiffer, Z. (2021). Period tracking app settles charges it lied to users about privacy. Retrieved July 20, 2021, from https://www.theverge.com/2021/1/13/22229303/flo-period-tracking-app-privacy-health-data-facebook-google

Schwöbel-Patel, Christine. 2017. The political economy of global constitutionalism. In Anthony F. Lang and Antje Wiener (eds.), Handbook on Global Constitutionalism. Cheltenham, UK: Edward Elgar Publishing.

Shetty, S. (2018). Decolonising human rights. Speech presented in London School of Economics, London. https://www.amnesty.org/en/latest/news/2018/05/decolonizing-human-rights-salil-shetty/

Shipp, L. & Blasco, J. (2020). How private is your period?: A systematic analysis of menstrual app privacy policies. Proceedings on Privacy Enhancing Technologies, 2020(4), 491-510. doi: https://doi.org/10.2478/popets-2020-0083

Singer, N. (2019). Period-tracking apps say you may have a disorder. What if they're wrong? Retrieved from https://www.

nytimes.com/2019/10/27/technology/personaltech/health-apps-hormonal-disorder-pcos.html

Stewart, C. (2021). Worldwide femtech market size 2027. Retrieved December 01, 2021, from https://www.statista.com/statistics/1125599/femtech-market-size-worldwide/

Tisné, M. & Schaake, M. (2018). The data delusion: Protecting individual data is not enough when the harm is collective. Retrived December 06, 2021, from https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/the_data_delusion_formatted-v3.pdf

Tyers, A. (2021). Oky: Co-created with girls, for girls. UNICEF. Retrieved December 06, 2021, from https://www.unicef.org/innovation/stories/oky-co-created-girls-girls

UN Economic and Social Council. (2016). General comment No. 22 (2016) on the right to sexual and reproductive health (article 12 of the International Covenant on Economic, Social and Cultural Rights) Retrieved December 06, 2021, from http://docstore.ohchr.org/SelfServices/

UNCTAD. (2021). Digital Economy Report 2021. Retrieved December 06, 2021, from https://unctad.org/webflyer/digital-economy-report-2021

United Nations Population Fund. (1994). Cairo Declaration on Population & Development. Retrieved December 07, 2021, from https://www.unfpa.org/resources/cairo-declaration-population-development

Weinberg, L. (2017). Rethinking privacy: A feminist approach to privacy rights after Snowden. Westminster Papers in Culture and Communication, 12(3), 5-20. doi: https://doi.org/10.16997/wpcc.258

WHO. (2021). Health Data as a global public good – a call for Health Data Governance 30 September. World Health Organization. Retrieved December 07, 2021, from https://www.who.int/news-room/articles-detail/health-data-as-a-global-public-good-a-call-for-health-data-governance-30-september

Zachariah, P. (2021). Why we need femtech. Retrieved December 02, 2021, from https://lifestyle.livemint.com/health/wellness/why-we-need-femtech-111620649640927.html

Zuboff, S. (2019, January). Surveillance capitalism and the challenge of collective action. In New Labor Forum, 28(1), pp. 10-29. SAGE Publications.