

Caring for Intimate Data in Fertility Technologies

MARYAM MEHRNEZHAD*, School of Computing, Newcastle University, UK

TERESA ALMEIDA, Department of Informatics, Umeå University, Sweden

Abstract: Fertility tracking applications are technologies that collect sensitive information about their users i.e. reproductive potential. For many, these apps are an affordable solution when trying to conceive or managing their pregnancy. However, intimate data are not only collected but also shared beyond users knowledge or consent. In this paper, we explore the privacy risks that can originate from the mismanagement, misuse, and misappropriation of intimate data, which are entwined in individual life events and in public health issues such as abortion and (in)fertility. We look at differential vulnerabilities to enquire data's vulnerability and that of 'data subjects'. We introduce the General Data Protection Regulation (GDPR) and how it addresses fertility data. We evaluate the privacy of 30 top 'fertility apps' through their privacy notices and tracking practices. Lastly, we discuss the regulations and fertility data as critical to the future design of tracking technologies and privacy rights.

CCS Concepts: • **Human-centered computing** → **Interaction design**; • **Security and privacy** → **Social aspects of security and privacy**; *Human and societal aspects of security and privacy*.

Additional Key Words and Phrases: Intimate data, privacy, women's health, public health, GDPR

ACM Reference Format:

Maryam Mehrnezhad and Teresa Almeida. 2018. Caring for Intimate Data in Fertility Technologies. In *TBC*. ACM, New York, NY, USA, 17 pages. <https://doi.org/10.1145/1122445.1122456>

1 INTRODUCTION

Data tracking related to fertility is not new, and women¹ have long tracked their intimate data, such as menstrual cycle or basal body temperature, to facilitate or prevent pregnancy [38]. Some approaches to doing so include the fertility awareness method (FAM), in which a woman would take her temperature, monitor her cervical mucus, and/or chart her menstrual cycle on a daily basis while keeping a record on paper, or hormonal contraception i.e. the pill. In recent years, fertility has gone digital and fertility tracking applications (apps) now proliferate and have hundreds of millions of users globally. Unlike menstruation apps, which include a wider variety of features and target a larger segment of the population, fertility apps are dedicated to potential fertility.

In HCI, there is a growing body of research dedicated to exploring fertility apps and technologies, for example in the design of sensor-enabled Internet of Things (IoT) devices. On the one hand, these have been mainly associated with menstrual (self-)tracking applications, to broaden understandings of the menstrual cycle or promote menstrual literacy [66], in ways that make menstrual tracking applications to seemingly focus on fertility or contraception. Such an instrumental approach to

* Authors contributed equally to this research.

¹This paper covers a set of literature that discusses ciswomen in their diversity and their use and experiences with fertility data. At the time of writing and best of our knowledge, and while a key element of data justice, studies on transgender and non-binary reproductive choice and (digital) fertility tracking are lacking or not readily available.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

TBC, TBC, TBC

© 2018 Association for Computing Machinery.

ACM ISBN 978-1-4503-XXXX-X/18/06...\$15.00

<https://doi.org/10.1145/1122445.1122456>

menstruation prescribes “the forms of knowledge and types of relationships with their body” those who menstruate are regarded as likely to embrace [26], opposed to how these technologies could exist differently in ways that would “encourage self-knowledge and affirm and support the needs of different kinds of menstruating bodies” [24]. On the other hand, some have specifically looked into fertility from a holistic viewpoint [13] to advance collaborative and supportive approaches [15] and dealing with emotions [14], attended to fertility tracking apps (FTAs) [66], infertility in men [56], through to ovulation tracking devices that aid conception [31]. Generally, these technologies seek to support conception, and individuals can record “menstruation and bodily signs of ovulation with the promise of producing more detailed knowledge of the individual’s menstrual cycle and predictions of their most fertile days or fertile window in the cycle” [29]. Used as reproductive technology, fertility tracking apps may be adopted by those who for the most part want to become pregnant as they actively facilitate pregnancy (ibid). Nonetheless, some have also highlighted how these tracking apps can offer inaccurate predictions which in turn have already led to numerous unwanted pregnancies and lawsuits [66]. Tracking is often about where one is heading in life [63], and whether fertility tracking is used for planning or preventing pregnancy as the ultimate goal, such technology is likely to have a positive impact on e.g family planning. However, the sociocultural construction of fertility impacts, among other, the wellbeing and safety of people in gender-specific ways and can lead to gender-based reprisals. For example, and while associated with various aspects of women’s health, (in)fertility can lead to experiences of discrimination or prejudice across-cultures and between the sexes [10]. Similarly, abortion is yet another topic of taboo involving fertility which intersects with issues around gender, class, race, religion, ability and health and which intersecting inequities can serve to prevent some from exercising their rights to safe abortion, as well as their right to continue a pregnancy and parent a child [44].

In this paper, we address the commodification of women’s personal and intimate data in fertility apps. Data commodification entails an increasingly economic perception of data, which encourages, ‘nudges’, obliges or coerces people “into using digital devices for monitoring aspects of their lives to produce personal data which can then be used for the purposes of others” [41]. These data circulate often for commercial profit and can be reappropriated for a range of purposes and by a range of actors and agencies [42]. These data are messy and complex, unregulated, and are not neutral or objective. It is also not clear who has the rights to these data, or who could legally access them. Indeed, research shows that there is a lack of clarity in the law in relation to this extremely sensitive data that include ovulation, sex activity, or medical records [68]. This can be observed on different levels e.g. user consent and third party sharing which may lead to malicious purposes, and that technologies fail to abide by the new General Data Protection Regulation (GDPR) in that they continue to share valuable personal information to commercial entities in ways of which users may not be fully aware [43]. Women may be aware of and have consented to some of these uses as agreed on or requested when first using the chosen app, but have no knowledge of others (such as some sensors on their devices and tracking data) [47]. In other words, as ‘fertility goes digital’ (valued at USD50 billion by 2025 [70]), it comes at the expense of (mostly) women’s privacy.

We position our approach as that of a much needed feminist view on data [7, 18, 25, 72]. We introduce the GDPR and explore how the GDPR interprets fertility data and how these have been addressed in the law. Fertility data covers a wide range of sensitive information which currently falls under ‘special category data’ as defined in the GDPR. Through the evaluation of existing privacy notices and tracking practices within 30 commercially-available at no cost fertility apps, we highlight how this category of personal information and intimate data is governed. We contend that feminist data practices that strive e.g. for consensual collection of data are critical when designing and developing fertility technologies. We contribute to ongoing research on women’s health in HCI and feminist approaches to data privacy.

2 BACKGROUND AND RELATED WORK

In this section, we overview the meanings of (in)fertility through present-day, and how it manifests differently depending on socio-cultural, economic, religious or political settings and viewpoints. Then, we consider fertility (self-)tracking technologies and how these entail the gathering of sensitive and intimate data which while relevant to the self also risk autonomy, to be harmful or potentially life-threatening.

2.1 The (In)Fertile Body

The World Bank reports that the total fertility rate is decreasing, just as age at first child birthing is increasing [6]. The vast majority of industrialized countries, where populations are projected to decline dramatically over the next 50 years [51], show a decline in fertility rates for reasons as varied as the economy or income, or improved education which strengthens knowledge and contributes to the economic empowerment of women [32]. In the UK, fertility rates have been decreasing, the average age of mothers increased, and women aged forty and over show higher fertility rate comparing to women aged under twenty, the latest release from the Office for the National Statistics shows [12]. Understanding one's fertility window entails having accurate information about fertility health, including options of preserving fertility, such as assisted reproductive technologies. Effects of fertility education on knowledge, desires and anxiety among the reproductive-aged have been discussed in [45], which highlights concerns regarding the physiological impact of learning about possible fertility issues, and related decision-making strategies. For example, [67] recognizes how lifestyle factors, such as smoking, or health issues, such as thyroid problems, can have an impact on the menstrual cycle and therefore on fertility.

While changing views on reproduction may have led to declining fertility rates (mostly) in the West, the socio-cultural implications of fertility can manifest in different ways. From abortion, pregnancy redundancy, through to intimate partner violence (IPV), the influence of cultural and gender practices on fertility drive e.g. gender-based violence (GBV) and domestic violence that have been shown to have significant associations with individuals and couples suffering from unwanted childlessness or involuntary infertility [54]. Moreover, a conservative family-oriented society anticipates that woman, during her utmost fertile years and in partaking in a heteronormative relationship, will experience pregnancy/childbirth [36]. The stigma associated with infertility and its costs i.e. physical, psychological, emotional and financial can manifest in a myriad of ways and traverse the able-bodied individual, people with disabilities and/or with conditions known to cause significant fertility issues. Moreover, the framing of infertility as a disability has been acknowledged in [54], but also serving as a basis to demand that infertile women achieve equal access to the financial resources to attain treatment [69].

Perspectives on reproduction and infertility through the ages might have changed, and technological advances that support reproductive choice and control over fertility have changed the way we think about the body. Nonetheless, infertility stigma persists and in this paper we explore the ways fertility self-tracking apps can inflict harm when characterizing the body in its experiences of infertility and fertility differentials.

2.2 What is Critical about Fertility Data?

Fertility apps have hundreds of millions of users globally, and for the most part are considered low-cost, tech-based ways to help their users conceive and to measure fertility. Fertility tracking involves users in putting in their personal and utmost intimate information on a daily basis e.g. temperature, mood, sexual activity, orgasm, cervical mucus, in addition to medical records. As more individuals increasingly use and interact with their intimate health data, what surfaces is a

growing number of popular accounts advancing how data is being stored on commercial platforms, sold to third parties or shared with one's employer [30, 61]. Women may be aware of and have consented to some of these uses, but have no knowledge of others [42]. A recent study shows how, despite growing popularity, evidence to inform the use of these apps is lacking, with little to no fertility specialist input during their development, and that regulation is sparse [19].

As noted in [68], applications developed by companies that focus on women's digital health seem to demonstrate a better understanding of the sensitivity of the data handled, and to respond accordingly with their policies and practices. Privacy and data protection issues are concerns in 'FemTech', a category referring to software, products, and services that advance women's health but that also stresses the commercial value of female technologies [64]. Data collection and privacy policies in fertility tracking, and/or what developing companies say is done with the data submitted, has been explored in [62], as well as how the data is used, and how, where, and who has developed the apps. Concerns are many and relevant to this paper are those which involve data privacy and the sharing of data with mostly invisible third parties, including medical clinics and research centres (ibid).

Furthermore, fertility data is not neutral in relation to gender, sexuality, and race. As noted in [68], developers seem to understand period and sexual data "as simply another piece of data rather than health data that is sensitive in nature". Being 'sensitive', we argue, involves defining and attending to the necessary privacy policies while taking into account ethnic, cultural, geographic and age diversity, in ways that are free of commercial influence [19]. The implications of tracking fertility are manifold and can come with adversity in relation to health or women's human rights. One such case is that of abortion. Data regarding the use of mobile technology for women seeking or receiving abortion is lacking [58], nevertheless, it has been reported how anti-abortion groups are using location tracking technology and spreading misinformation, a situation that becomes more alarming as there is an increased reliance on online tools and/or closure of clinics after COVID-19 [48]. As the access to sexual and reproductive healthcare is lost due to the coronavirus pandemic (with not only unsafe abortions but also unintended pregnancies and maternal deaths expected to increase in numbers), many worldwide are being 'stripped of their rights' as disruptions to family planning and contraception services become the unfortunate norm.

Managing fertility, i.e. being able to choose whether, when, and how often to get pregnant and have a child [65], is critical. In the following section, we discuss a series of life-course events that are impacted by fertility and highlight how data exploitative technologies being developed for its management can be harmful and socially exclude, oppress and marginalize individuals/communities.

3 DIFFERENTIAL VULNERABILITIES IN FERTILITY TRACKING

Differential vulnerabilities is "a concept that recognizes how different populations face different types and degrees of security and privacy risks" [59]. Vulnerability is a concept used across different disciplines e.g. bioethics or psychology [17], and a current and functional definition in science covers "three dimensions: *exposure* to hazard, *susceptibility* i.e. effect of exposure and *capacity of response* by coping and adaptability" [17]. In HCI, the notion of differential vulnerabilities has been introduced in [59] to discuss cybersecurity and privacy as perceived in a series of toolkits available to users and to critically reflect on the security and privacy needs that are not met. While doing so, it also asks whom these toolkits are suited for and who is designing or funding them and to what ends, thus challenging the universalizing tendencies that frame cybersecurity and privacy around an abstract or generic user [22]. Specific to this paper, we explore the privacy risks that can originate from the mismanagement, misuse, and misappropriation of intimate data. For example, in [37] we are introduced to the concept of socio-cultural data traps, technologies that 'by design' deliberately limit the possibility of letting go of their 'data subjects' by making it difficult to e.g.

opt-out of data sharing during app use or even after uninstalling the app. The option of opting-out is, as we will discuss further in the next section, a legal requirement, a technical possibility, and a human/user right. We highlight the mismanagement, misuse, and misappropriation of highly sensitive and intimate data such as that collected in fertility technologies to shed light on data's vulnerability and that of 'data subjects'.

3.1 Potential Risks

Privacy risks in intimate data relate to the fact that data are typically collected by, and stored on, non-intimate commercial platforms [38]. While data may appear to be available only to the user or shared only within an intimate partnership, data may also be shared with or sold to third parties, e.g. app developers or advertisers (ibid). For the most part, these are connections established via fine-print privacy policies and terms-of-service agreements and, while technically permissible under such terms, violate user expectations and contextual norms. Such data-sharing practices abound and, while the 'data subject' might be asked to give their consent prior to the gathering and processing of their data [72], it is less clear how well that individual consent is informed consent or what exactly will happen to the data gathered afterwards.

Relevant to this paper is a series of life-course events that impact the health and wellbeing of a vast number of people, and which fertility tracking privacy and security have shown to impact at multiple contextual levels including in reproductive health, rights and justice. To illustrate our argument, we highlight the following three data cases: abortion, infertility, and pregnancy.

3.1.1 Abortion: Fertility tracking apps and abortion have a controversial history. Events include those which target women to mine and exploit their data e.g. the case of an ideologically aligned fertility app that was funded and led by anti-abortion, anti-gay Catholic campaigners [27]. In exploiting a vulnerability, that which implies preventing women from getting the care they need e.g. by misleading them into believing in wrongful or undesired information, or by misusing their data, abortion tracking mechanisms implemented via period/fertility apps are a reality that has been harmful to many. While abortion restrictions differ worldwide and reasons for seeking an abortion are particular to each one individual, accounts that range from tracking the menstrual cycles of migrant girls in the USA [5] through to fallacious apps with an agenda based on religious beliefs or other, all share the same goal which is to prevent anyone who chooses to terminate their pregnancy from accessing the care they need. In other words, the misappropriation of data can expose and make susceptible the individual who might be more or less able to cope depending on the context, e.g. an unaccompanied minor under the custody of the Office of Refugee Resettlement custody who would find herself deprived of her reproductive rights, or the case of an ovulation-tracking app whose system not long ago has been reported to allow anyone to access the user's health data, including whether she had had an abortion [9]. Furthermore, pregnancy loss, a loss due to stillbirth or miscarriage, if to occur it cannot be prevented. It is a stigmatized life event known to cause distress or trauma to those who experience it [69] and one which some can be prosecuted for [76].

3.1.2 Infertility. Fertility apps also aim (and target) those who are initiating fertility treatment. They can track their cycles and input treatment i.e. such as in vitro fertilization (IVF), or other fertility-related event e.g. egg freezing, surrogacy or egg donation. As reported by the World Health Organization, key issues around infertility include e.g. mental health, stigma or violence [54]. While fertility decreases for a myriad of reasons [32], infertility has also become less stigmatized. Nonetheless, cultural and gender practices that inform and influence fertility e.g. the social/cultural constructions of motherhood still impact many, causing e.g. disruptions to their sense of self, economic hardship, shame and blame, and sometimes violence. In fact, intimate partner violence (IPV), gender-based violence (GBV) and domestic violence have been shown to have significant

associations with individuals and couples suffering from unwanted childlessness or involuntary infertility [54]. Furthermore, and had mentioned earlier how data may appear to be available only to the user but also shared within an intimate partnership, the latter with or without permission: when an intimate partner has access to data for which they do not have consent, how would such a breach of privacy work in the context of infertility and IPV? In exploiting a vulnerability, that seen in e.g. cases of intimate partnerships regarding sharing of non-consensual data, data that leaves one partner exposed and for that emotionally and/or physically vulnerable and likely limited in resources to counteract, fertility and reproductive health tracking needs to change so not to legitimize such circumstances. Another example would be that of discrimination in the workplace due to infertility as discussed in [73].

3.1.3 Pregnancy. While some might use fertility tracking apps for pregnancy prevention, it is likely that those using them are interested in getting pregnant. Different from menstruation apps, fertility apps are dedicated specifically to reproductive potential. In popular science outlets, cases of success abound. For instance, when a user is said to have successfully used an ovulation-tracking bracelet, one that is “worn at night and uses data from a woman’s heart rate, skin temperature and other key physiological parameters to figure out when she will be most fertile in any given month” [8], after suffering secondary infertility or miscarriage [49]. What is also reportedly happening is that of some fertility and pregnancy technologies sharing their user data without their permission [61], to third parties or including employers [30]. How and if these data can benefit health care is disputed, as much as is how such a move could contribute to affecting one’s career or job prospects. For example, pregnancy redundancy in the workplace as long been an issue for women, including in the UK where pregnancy-related discrimination still fails to guarantee effective job-protections i.e. not being terminated or demoted due to taking parental/maternity leave [2], or as seen in the case of a female Iranian parliament member who was attacked on social media after she announced the birth of her child [23]. Internet users accused her of hiding her pregnancy during her campaign and blamed her for using public funds during her maternity leave.

3.2 Fertility Data in the Law

In recent years, a few different data protection regulations have come into effect including the General Data Protection Regulation (GDPR)[74], the California Consumer Privacy Act (CCPA) [16], and the Chinese Personal Information Security Specification (PISS) [57]. In this paper, we will expand on the GDPR only and focus on how this law addresses fertility data to initiate a critical-reflective research practice in this space. We use guidelines set by the Information Commissioner Officer (ICO), the independent regulatory office (national data protection authority) dealing with data protection regulations including the GDPR across the UK.²

Personal data is defined as: “information that relates to an identified or identifiable individual” [33]. The GDPR highlights some types of personal data as likely to be more sensitive and gives them extra protection [34]. This data includes the information that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, as well as genetic data and biometric data, and, last but not the least, data concerning health, sex life, and sexual orientation. These categories of data are referred to as ‘special category data’. The GDPR prohibits the processing of special category data with 10 exceptions to this general prohibition: explicit consent, employment, social security and social protection (if authorised by law), vital interests, not-for-profit bodies, made public by the data subject, legal claims or judicial acts, reasons of

²ICO’s mission is to “uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals” (ico.org.uk). The ICO translates the legal documents to technical language helping the technology developers to provide law-compliant solutions.

substantial public interest (with a basis in law), health or social care (with a basis in law), public health (with a basis in law), and archiving, research and statistics (with a basis in law). Special category data cannot be used for solely automated decision-making (including profiling) that has legal or similarly significant effects unless there is explicit consent or substantial public interest conditions are met. This requirement is on top of all the other subject rights for general personal data [52].

When we search in the GDPR articles and guidelines (e.g. provided by ICO), fertility-related data is not mentioned directly. Naturally, one would assume that fertility-related data falls under health and sex life data. The GDPR defines health data as “data concerning health’ means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status” [52]. Though, it does not define ‘data concerning sex life’ in the way it does for health data.

A few more focused guidelines and documents have been developed around the special category data including the European Data Protection Board (EDPB)’s guidelines for genetic data [20] and biometric data [21]. However, to the best of our knowledge, there don’t exist any specific data protection regulations set for ‘fertility data’ when collected and processed beyond health and medical clinics [11, 28, 50]. This ambiguity in the law can lead to undesirable outcomes and cause serious risks to those using these technologies, as discussed in the previous section.

4 AN EVALUATION OF APP PRIVACY NOTICES AND TRACKING PRACTICES

In this section, we analyse top fertility apps for their privacy notice practices and the actual tracking behaviours. In doing so, we aim to show how the data concerning these technologies are dealt with when not handled by health and medical professionals in clinics. More specifically, we want to find out how popular fertility apps deal with this data i.e. considering them special category data, general personal data, a combination of both, or neither. We focus on analysing fertility apps within the GDPR framework since we download our apps from the Google Play App Store UK which is complying with the GDPR.

4.1 Methods and Tools

4.1.1 Apps Set. We study Android apps since they are easily downloadable and many tools exist for analysing their tracking practices. All apps were downloaded from the Google Play Store on a Google account which was already in use on a smartphone (Android ver: 9) to simulate real-world experiments. As our case study, we searched the word “Fertility” in Google Play (UK) in August 2020 via Incognito Mode on Google Chrome. The top 30 apps returned by our search were chosen as the apps set of this study (see Appendix). This is the same number of apps studied in [68] for Period trackers and will allow us to carry out our manual analysis. We took a different approach as of [3, 68] in our app selection and did not filter the apps based on the numbers of installs and user ratings for the following reasons: (1) fertility-related apps generally have a lower number of installs than period-related apps since they have a more focused set of audience, (2) some of these apps are new in the market and have a fewer number of downloads, but their popularity is on the rise, and (3) excluding the apps with a lower number of installs (e.g. less than 100K as proposed in [68]) would discriminate thousands of users of a certain subset of fertility apps (e.g. those for communication and social purposes). Therefore, we decided to include all the top apps returned by our search in order to conduct an inclusive study.

4.1.2 GDPR requirements: To satisfy the GDPR’s data protection principles, rights and obligations, the online service providers are required to tell people that the tracking technologies (including cookies) are there, explain what these technologies are doing and why, and get the person’s consent

to use the tracking data. The ICO [33] provides extensive guidelines on law-compliant practices as follows. The service providers are required to present a consent to the user when they first visit the service. This consent must involve some form of unambiguous positive action (such as ticking a box and clicking a link). This consent should be separated from other matters (e.g. terms and condition and privacy policy). In order to avoid ‘nudge behaviour’, the privacy consent should allow the user to make a choice, therefore it should include options such as *Accept (Yes, Agree, Allow, etc.)* and *Reject (No, Disagree, Block, etc.)*. If a privacy notice only includes *Accept* and requires the user to engage with the notice and accept the settings before they can access an online service’s content, they are presenting the user with a tracking ‘wall’. Such user consent is not considered valid, if the use of this tracking wall nudges the user to agree to their personal data being used by the company or any third parties as a condition of accessing the service. Similar to the above, the consent should not highlight *Accept* over *Reject* and other options. The online services should enable the user to withdraw the previously given consent with the same ease that they gave it. The service providers should not rely on the other control mechanisms (e.g. browser settings or mobile settings) as users’ opt-out mechanism. Pre-enabling the non-essential tracking technologies without user taking a positive action before it is set on their device does not represent a valid consent and is a violation.

4.1.3 Privacy Notice Analysis: In order to analyse the privacy notice of our case study apps, we install each app and open it on our Android device. We observe whether there exists a privacy notice when the app is opened for the first time (and further visits), how this notice is presented (consent wall, blended, etc.), and what is the content of this notice. In some apps, users can familiarise themselves with the app via a few introduction pages leading the user to the actual first page. We either skip this or, where not possible, click next. Some apps ask for particular permissions (e.g. location, photos, notification) or settings (e.g. make lists, choose service preferences), we reject them all -unless required to be able to open the app. Note that some apps need the user to log-in or sign-up before providing any services. If we cannot continue as a guest, or observe any privacy notice/link through the sign-up pages with the app’s default settings (and before creating an account), we don’t log-in. Therefore, we don’t observe whether there exists any privacy notice beyond the log-in page. In each Android app, we analyse the user consent notice to identify the user control options. After extracting the options and listing them, we categorise them based on the choices they give to the user (e.g. agree or reject, agree or further options, available links, no option). We compare these practices against the recommended guidelines provided by the Information Commissioner’s Office (ICO)’s guidelines [33].

4.1.4 Tracking Practices Analysis. In order to observe the tracking behaviour of apps, we use Lumen Privacy Monitor app (ver 2.2.2) [60] (a privacy-enhancing free Android app) to analyse each app’s traffic and communications. Lumen reveals how each app communicates with tracking services and list the level of the sensitivity of the shared data (device model, fingerprint, etc.). Lumen doesn’t require root permissions and leverages the VPN API on Android. We install Lumen on our Android device and allow all the permissions and the VPN request. Then we open the apps and leave them in the background for an hour while carrying on with the normal usage of the mobile device. We don’t interact with the app (i.e. no click, no log-in, no scroll, etc.). Note that we don’t interact with the privacy notice for the purpose of this study, and just let the app be open for an hour while carrying on with the normal usage of the mobile. We report the contacted domains and identified trackers by Lumen for each app. Our approach is in line with the one adopted by [46] for studying the tracking practices of Android apps in real-world. Though, since this approach only reflects the tracking behaviour of our case study apps before interacting with the privacy notice (and generally engaging with the app), we also study the available trackers in these apps through a static analysis

Status	No. of apps
No privacy-related content	12 (40%)
Embedded in sign-up and or terms and condition pages	13 (43%)
Dedicated privacy notice wall	4 (13%)
Dedicated privacy notice with other options	1 (3%)

Table 1. Privacy notice status of Fertility apps

tool. We use Exodus Privacy app (a privacy audit platform for Android apps)³ to find the number and types of trackers within each app. Exodus uses static analysis (the evaluation of the app code without executing it) to find the tracker’s code signature in an app’s APK [1].

4.2 Results

In this section, we present the results of the analysis that we performed on the privacy notices of these apps in accordance to the GDPR and the ICO’s guidelines. In addition, we demonstrate the actual tracking behaviours of these apps in practice.

4.2.1 Privacy Notice. We observed (as shown in Table 1) that 12 out of 30 apps did not present any privacy-related content (e.g. banner and links) to the user when opened for the first time and on the later visits. 13 of our apps included privacy-related content (e.g. description, boxes to tick, and links) within their sign-up pages and/or embedded with other terms and conditions. Five apps had a dedicated privacy notice where four of them presented the user with one option only: Accept, while the remaining one highlighted Accept over Reject (Fig. 2, left). We found no app in our case study set which presented the user with a privacy notice containing Accept and other options (e.g. reject and/or settings) where Accept was not highlighted over other options. According to ICO’s guidelines [33], a consent mechanism that doesn’t allow a user to make a choice or highlight Accept over Reject represents a non-compliant approach; a practice which was seen in five of our apps. It also says that consent cannot be bundled into terms and conditions and it must be separate from other matters; another non-compliant practice which was observed in 13 apps. All these 18 apps have taken a ‘take it or leave it approach’ which is considered inappropriate where the user has no genuine choice but to accept. The other apps did not include any privacy notice at all.

4.2.2 Tracking Practices. As can be seen in Fig. 1, the majority of these apps contain trackers and a lot of them start tracking the user once the app is open. An example of the reported trackers and domains by Lumen as well as those returned by Exodus for one of our Fertility apps are shown in Fig. 2. Except for five apps, Lumen could analyse all the other apps in our set. It detected at least one tracker for 15 apps (out of 25) – 3.8 trackers on average. Note that these trackers were detected while these Fertility apps have been running in the background and under the test condition that no prior privacy settings have been done by the user. An example of such trackers is shown in Fig. 2, middle. Although the exact shared data of these apps (e.g. sexual activities and medical records) with trackers are not reported by Lumen (dynamic analysis is required [39]), it can still report general privacy leaks. Lumen detected at least three privacy leaks by these apps including the Build Fingerprint (which is a value that identifies uniquely the Android OS and its version), Device Model (which identifies the device model and manufacturer), and Time-zone (which in this case was Europe/London and can help to locate the user geographically). As stated by the Lumen app,

³reports.exodus-privacy.eu.org/en/

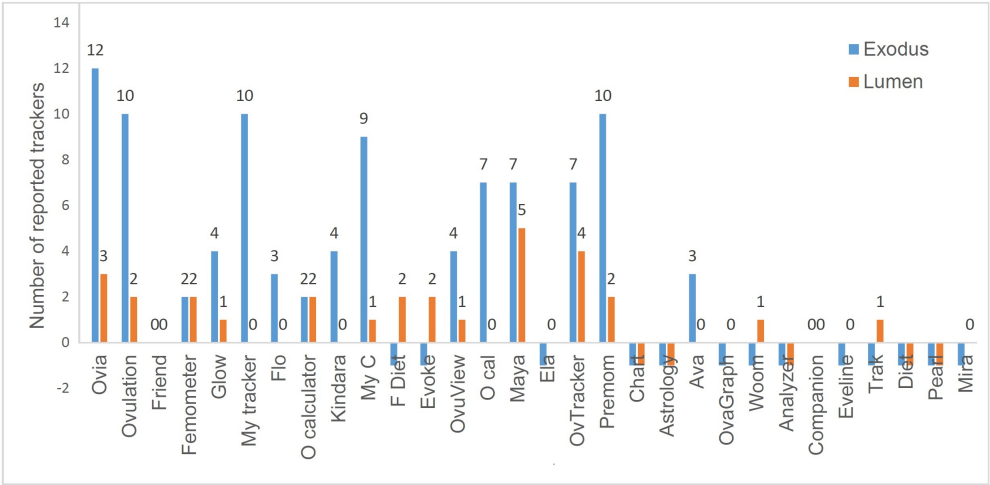


Fig. 1. The number of trackers reported by Exodus (static analysis) vs. Lumen (before interacting with the privacy-related content). -1 means no report was available by these tools for the app.

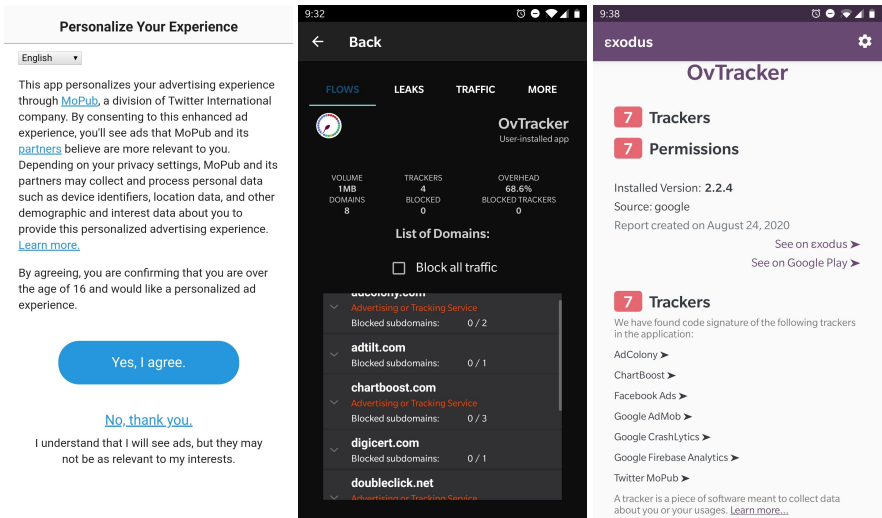


Fig. 2. The trackers detected by Exodus (right), Lumen (middle) for a Fertility app in the presence of the privacy notice (left) and before any user interaction with it. This was the only app in our set which presented a privacy notice with more than one choice to the user. Yet it highlighted Accept over Reject (non-compliant approach).

this information, specially when combined with other leaks, can reveal more information about the user’s personality, preferences, wealthiness, and demographics.

As it can be seen in Fig. 1, Exodus has reported a higher number of trackers in comparison to Lumen – 5.5 trackers on average. This was expected since Exodus analyses the entire app code as opposed to the app behaviour under a particular test condition. 13 of our apps haven’t been analysed by Exodus yet (and it did not necessarily correlated with the number of installs). Out of

the remaining 17 apps, Exodus detected at least two trackers within each app, except for two apps where no trackers were identified. An example of such trackers is shown in Fig. 2, right.

In a recent study [46], we have shown that the number of trackers on 101 Android apps corresponded to top EU websites is 2.6 on average. We have performed our experiments under the exact same test condition (privacy tools, Android version, no interaction with the privacy notice, etc.). When looking at the app list in [46], we find no app directly linked to special category data. Yet, we find more trackers in our study in comparison to apps of popular general websites (3.8 vs 2.6). In addition, previous research has pointed out that there are gender-based differences in privacy protection behaviour [55], where men tend to be more familiar with various privacy protection methods and use them more often than women do [53]. The above raise concerns in relation to handling fertility data via free apps given that most parts of these data are more sensitive.

4.3 Limitations

4.3.1 App Set. In this study, we adopt a general approach to choose our apps. We don't filter the apps based on factors such as the number of downloads and user rate and, in doing so, we take an inclusive approach as mentioned before. Also, we search the word 'Fertility' only, and do not include other keywords such as Ovulation, Fertility Tracker/Calculator, Pregnancy, Menstruation, Period, etc. This approach is by choice since building a keyword set can be debatable and may lead to a different set of apps which do not directly deal with fertility data. In addition, we believe that regardless of the app set, the results can be generalised. In other words, what we have demonstrated in this paper is a snapshot of the serious problems concerning intimate data in fertility technologies. We consider that extending the data set by including more apps (including iOS apps) and platforms (e.g. IoT) and searching more keywords will result in more confident results, and we plan to do that in the future.

4.3.2 Tools. We study our apps by using two privacy-enhancing tools (Lumen and Exodus). While these tools can reveal the trackers that these apps share data with, they have certain shortcomings. Exodus's app set is continuously being updated and did not include some of our apps. In addition, when we run Lumen on Android 7 or later (which is the case in this study), it will not be able to monitor most TLS/HTTPS connections due to the limitations imposed by Google on how certificate stores are trusted. These limitations may have caused a lower number of detected trackers in their reports. Yet, we observed that the majority of these apps contain trackers and, without waiting for the user privacy choice, they would track the user. We plan to extend our privacy analysis by going beyond the first page of the app (e.g. by simulating user interaction to input data) to reveal even more privacy leaks and via more advanced methods e.g. dynamic analysis [39].

5 DISCUSSION

Differential vulnerabilities in intimate data show the complexity of privacy as a universal right. In our exploration of tracking practices and app privacy notices in fertility technologies, we found that the standard practices can easily violate the law. In this section, we discuss the current regulations and intimate data practices as critical to the future design of fertility-tracking technologies.

5.1 Ambiguity and Complexity of Fertility Data

In exploring how the GDPR interprets fertility data and how these have been addressed in the law, we found different levels of ambiguity, which become even more serious when taken into the implementation level. The app categories of our use case apps (see Appendix A) suggest that most of these fertility apps are classified as 'Health & Fitness', a few as 'Medical', and one as 'Communication'. Miscategorising an insecure app which contains medical records (such as

user's medical conditions and/or medicines) as Health & Fitness would enable the developers to avoid the potential consequences, for example, of remaining in the app market without drawing significant attention to it [71]. At the time of this writing, Google⁴ defines Health & Fitness category examples as "Personal fitness, workout tracking, diet and nutritional tips, health & safety, etc." and Medical as "Drug & clinical references, calculators, handbooks for health-care providers, medical journals & news". At the time of the app registration in the app store, the developers have to select, based on their opinion and judgment, the most appropriate category. However, due to the ambiguity in the definition of different categories, the doors are open to potential misuse and gaming by the registrant. Although app categories can be refined periodically by the app store, app miscategorisation persists and it remains an issue to be dealt with [71].

We argue that the data collected by fertility apps (and other technologies) is a complex combination of health, medical, sex life and lifestyle – which may reveal e.g. religious and political views, or sexual orientation. For example, sexual activity during menstruation is prohibited in some religions and cultures. Such patterns would easily show in fertility records. Our findings show how the mismanagement and misuse of fertility-related data can seriously put users of these technologies at risk. When considering differential vulnerabilities' three dimensions, we conclude that: (1) the exposure to hazard is high since the tracking behaviours are intrusive, (2) the effect of any exposure is serious since the data is sensitive and the users are not confident in protecting themselves, and (3) the capacity of response is limited due to the ambiguity and complexity of fertility data, as well as the lack of accountability and care in this space.

In addition, with extra processing and in combination with data collected by smart IoT devices, fertility data may also reveal biometric and genetic information. While some of this may also be present in similar apps (such as menstrual-tracking), the sensitiveness level and complex combination are unique to fertility technologies since mismanaging such data may affect the person's life significantly. In addition to the privacy of the user (as we discussed in Section 3), misusing such data can put others at various types of risks too. Fertility data also concerns collective privacy [40], that is, not only the user's personal privacy, but also that of her/his/their contacts, connections and relations, and the privacy of co-constructed personal information – which is possible through these technologies. Reportedly, similar apps (menstrual-tracking) share sensitive data (e.g. sex activity) with third parties (e.g. Facebook) the moment the user opens the app, even without a Facebook account [35]. Similar reports have been appearing on the news many times in the last few years [61, 75]. In view of all the above, we believe that much more adequate, lawful, and ethical processes are required when dealing with this data.

5.2 Accountability and Care

Certainly, data that is sensitive needs to be handled ethically and lawfully or, otherwise, risks are plenty. Risks include that of data's vulnerability and of 'data subjects', as *making vulnerable* hints on exposure, having the capacity to respond or not, and/or being able to cope and adapt when data that is intimate and private surfaces in an undesirable manner. Moreover, differential vulnerabilities or how privacy risks might impact people differently and depend on a myriad of circumstances, matter. While experiences of discrimination or prejudice might not be intended in most of the technologies we discuss in this paper, it is also factual that some are designed for implicit biases or are deceptive. Within, lay a lack of regulation and clarity in the law that allows for more and more technologies to explore intimate data sets, eventually in settings that are prone to harm those who use them. Indeed, caught between the complexity of the data and the ambiguity in the law, the technical possibilities continue to grow, e.g. with AI. Nonetheless, the opportunities that are

⁴google.com/googleplay/android-developer/answer/113475?hl=en-GB

presented with developing capacity should also come with the responsibility to create a functional, meaningful and respectable collection of data within tracking practices. For example, as put in [68] in relation to the sometimes excessive number of data collection options, “even with the continuous advancements in machine learning today, it is highly difficult to see how a profile picture may improve the period tracking services offered by these kinds of apps.”

In arguing for feminist data practices, we contend that approaches to (specific to this paper) fertility tracking deem to impact – by supporting and improving – all human lives. We attend to this through a care-full and caring scope of the literature and a series of events that are real and represent contemporarity as we know it across the globe. Our study introduces a real-world viewpoint as an entry point to show how these are lacking in care-related technologies that are more or less accessible to many, and which many use on a daily basis. While embracing care in its complexity and political ambivalence, we see the potential and pitfalls of technologies that promote (self-)care, including that of fertility, which offer the individual an added or alternative way to manage their care and their conditions. Because data collected might misrepresent one’s health conditions, and context-free data is ripe for misinterpretation [18], considering context in relation to intimate data is critical. Future fertility technologies that aim to connect knowledge back to (in)fertile bodies should account for people’s particular (bodily) biographies and disruptions, and tools and devices to safeguard and advance equity and human rights. Moreover, use and experiences with fertility data are readily available in both academic contexts and popular science outlets that discuss ciswomen while studies on transgender and non-binary reproductive choice and digital fertility tracking are lacking. Fertility includes genders beyond the binary and non-binary fertility options need to be included in the design of these technologies.

Overall, reproductive health and rights is about access to e.g. abortion, but it is also the freedom to be a parent independently of sex or genders. We advocate for advancing justice and equity in fertility technologies in ways that, for instance, innovate and can be transferred with care to new contexts and concerns, that are more humanistic and inclusive, as discussed in [4]. In doing this, we aim for a future that seeks its technological and social innovations to be developed responsibly and transparently, the key to the process of social change.

6 CONCLUSION AND FUTURE WORK

In this paper, we link fertility tracking and related life events to explore privacy practices and the implementation (with)in the technology that circumscribe these varied experiences. In so doing, we illustrate how intimate data is or can be mismanaged, misused, and misappropriated, and therefore contribute to breaches of privacy that put people at risk. Specifically, we focus on fertility data and enquire into how this is exploited across socio-cultural, economic, or political and religious contexts. We study the GDPR to observe how fertility data has been addressed in the law. We conduct an empirical study in which we analyze 30 fertility apps for their privacy notice practices and their actual tracking behaviours. Our evaluation confirms that not only the privacy of the user is not respected by these apps through the appropriate measures designed for dealing with ‘special category data’, but also, that the general approach of these popular apps concerning user privacy lacks in obvious directions. Furthermore, this paper introduces a study concerning the design of the systems as opposed to the users; measuring the privacy practices of a certain set of apps. We believe that it is equally important to study users and seek understanding of their privacy concerns, preferences, and practices. Our future research will investigate users’ perception and practice of the available Privacy Enhancing Technologies (PETs) of fertility apps and IoT devices to expand to and benefit different communities by contributing to more humanistic and inclusive approaches in the design of privacy and security features of such technologies. We encourage other researchers to conduct similar studies across regulations.

REFERENCES

- [1] 2019. Exodus-Privacy. github.com/Exodus-Privacy (2019).
- [2] Maternity Action. 2019. Discrimination during maternity leave and on return to work. (2019). <https://maternityaction.org.uk/advice/discrimination-during-maternity-leave-and-on-return-to-work/>
- [3] Rajindra Adhikari, Deborah Richards, and Karen Scott. 2014. Security and privacy issues related to the use of mobile health apps. *ACIS*.
- [4] Teresa Almeida, Madeline Balaam, and Rob Comber. 2020. Woman-Centered Design through Humanity, Activism, and Inclusion. *ACM Trans. Comput.-Hum. Interact.* 27, 4, Article 27 (Sept. 2020), 30 pages. <https://doi.org/10.1145/3397176>
- [5] Priscilla Alvarez. 2019. House Judiciary Committee asks former ORR director to clarify testimony on pregnant minors. *CNN* (2019). <https://edition.cnn.com/2019/03/22/politics/scott-lloyd-pregnant-minors/index.html>
- [6] World Bank. 2019. Fertility rate, total (births per woman). (2019). <https://data.worldbank.org/indicator/SP.DYN.TFRT.IN?end=2018&start=2014>
- [7] Shaowen Bardzell. 2010. Feminist HCI: Taking Stock and Outlining an Agenda for Design. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Atlanta, Georgia, USA) (*CHI '10*). Association for Computing Machinery, New York, NY, USA, 1301–1310. <https://doi.org/10.1145/1753326.1753521>
- [8] Mandy Behbehani. 2019. Tech boom in fertility apps aids women struggling to get pregnant. *San Francisco Chronicle* (2019). <https://www.sfchronicle.com/style/article/Tech-boom-in-fertility-apps-aids-women-struggling-14261714.php>
- [9] Jerry Beilinson. 2016. Glow Pregnancy App Exposed Women to Privacy Threats, Consumer Reports Finds. *Consumer Reports at consumerreports.org/mobile-security-software/glow-pregnancy-app-exposed-women-to-privacy-threats/* (2016).
- [10] Linda Rae Bennett. 2016. Infertility and inequity across the globe. (May 2016). <https://doi.org/10.1080/17441730.2016.1176805>
- [11] European Commission. Accessed 2020. European Commission Standards for Medical Devices. https://ec.europa.eu/growth/single-market/european-standards/harmonised-standards/medical-devices_en (Accessed 2020).
- [12] David Corps. 2020. Births in England and Wales: 2019. 452 (2020). <https://www.ons.gov.uk/peoplepopulationandcommunity/birthsdeathsandmarriages/livebirths/bulletins/birthsummarytablesenglandandwales/2019>
- [13] Mayara Costa Figueiredo. 2020. Self-Tracking for Fertility Care: A Holistic Approach. In *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) (*CHI EA '20*). Association for Computing Machinery, New York, NY, USA, 1–9. <https://doi.org/10.1145/3334480.3375029>
- [14] Mayara Costa Figueiredo, Clara Caldeira, Elizabeth Victoria Eikey, Melissa Mazmanian, and Yunan Chen. 2018. Engaging with Health Data: The Interplay Between Self-Tracking Activities and Emotions in Fertility Struggles. *Proc. ACM Hum.-Comput. Interact.* 2, CSCW, Article 40 (Nov. 2018), 20 pages. <https://doi.org/10.1145/3274309>
- [15] Mayara Costa Figueiredo, Clara Caldeira, Tera L. Reynolds, Sean Victory, Kai Zheng, and Yunan Chen. 2017. Self-Tracking for Fertility Care: Collaborative Support for a Highly Personalized Problem. *Proc. ACM Hum.-Comput. Interact.* 1, CSCW, Article 36 (Dec. 2017), 21 pages. <https://doi.org/10.1145/3134671>
- [16] Lydia de la Torre. 2018. A guide to the california consumer privacy act of 2018. *Available at SSRN 3275571* (2018).
- [17] Finn Diderichsen, Johan Hallqvist, and Margaret Whitehead. 2019. Differential vulnerability and susceptibility: how to make use of recent development in our understanding of mediation and interaction to tackle health inequalities. *International Journal of Epidemiology* 48, 1 (2019), 268–274. <https://doi.org/10.1093/ije/dyy167>
- [18] Catherine D'Ignazio and Lauren F. Klein. 2020. Data Feminism. (2020).
- [19] Sarah Earle, Hannah R Marston, Robin Hadley, and Duncan Banks. 2020. Use of menstruation and fertility app trackers: a scoping review of the evidence. *BMJ Sexual & Reproductive Health*, Article bmjsrh-2019-200488 (2020). <https://doi.org/10.1136/bmjshr-2019-200488>
- [20] European Data Protection Board (EDPB). 2004. Working Document on Genetic Data. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2004/wp91_en.pdf (2004).
- [21] European Data Protection Board (EDPB). 2012. Opinion 3/2012 on developments in biometric technologies. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf (2012).
- [22] Serge Egelman and Eyal Peer. 2015. The Myth of the Average User: Improving Privacy and Security Systems through Individualization. In *Proceedings of the 2015 New Security Paradigms Workshop* (Twente, Netherlands) (*NSPW '15*). Association for Computing Machinery, New York, NY, USA, 16–28. <https://doi.org/10.1145/2841113.2841115>
- [23] BBC Farsi. 2020. Iranian social media reaction to female Parliament member gives birth to her child (Farsi). *BBC at bbc.com/persian/iran-features-5341846* (2020).
- [24] Sarah Fox and Daniel A. Epstein. 2020. *Monitoring Menses: Design-Based Investigations of Menstrual Tracking Applications*. Springer Singapore, Singapore, 733–750. https://doi.org/10.1007/978-981-15-0614-7_54

- [25] Sarah Fox, Noura Howell, Richmond Wong, and Franchesca Spektor. 2019. Vivewell: Speculating Near-Future Menstrual Tracking through Current Data Practices. In *Proceedings of the 2019 on Designing Interactive Systems Conference*. 541–552.
- [26] Sarah E. Fox, Amanda Menking, Jordan Eschler, and Uba Backonja. 2020. Multiples Over Models: Interrogating the Past and Collectively Reimagining the Future of Menstrual Sensemaking. *ACM Trans. Comput.-Hum. Interact.* 27, 4, Article 22 (Sept. 2020), 24 pages. <https://doi.org/10.1145/3397178>
- [27] Jessica Glenza. 2019. Revealed: women’s fertility app is funded by anti-abortion campaigners. *The Guardian* (2019). theguardian.com/world/2019/may/30/revealed-womens-fertility-app-is-funded-by-anti-abortion-campaigners
- [28] UK Government. Accessed 2020. Guidance on Medical devices: EU regulations for MDR and IVDR. <https://www.gov.uk/guidance/medical-devices-eu-regulations-for-mdr-and-ivdr> (Accessed 2020).
- [29] Josie Hamper. 2020. ‘Catching ovulation’: Exploring women’s use of fertility tracking apps as a reproductive technology. *Body & Society* (March 2020). <https://doi.org/10.1177/1357034X19898259>
- [30] Drew Harwell. 2019. Is your pregnancy app sharing your intimate data with your boss? *The Washington Post* (2019).
- [31] Sarah Homewood, Harvey Bewley, and Laurens Boer. 2019. Ovum: Designing for Fertility Tracking as a Shared and Domestic Experience. In *Proceedings of the 2019 on Designing Interactive Systems Conference* (San Diego, CA, USA) (DIS ’19). Association for Computing Machinery, New York, NY, USA, 553–565. <https://doi.org/10.1145/3322276.3323692>
- [32] Stefan Hutzler, C. Sommer, and P. Richmond. 2016. On the relationship between income, fertility rates and the state of democracy in society. *Physica A: Statistical Mechanics and its Applications* 452 (March 2016), 9–18. <https://doi.org/10.1016/j.physa.2016.02.011>
- [33] Information Commissioner Office (ICO). 2020. How do we comply with the cookie rules ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/how-do-we-comply-with-the-cookie-rules/ visited Sep 2020. (2020).
- [34] Information Commissioner Office (ICO). 2020. What is special category data? ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-is-special-category-data/ visited Sep 2020. (2020).
- [35] Privacy International. 2019. How Menstruation Apps Are Sharing Your Data. [at: https://privacyinternational.org/long-read/3196/no-bodys-business-mine-how-menstruations-apps-are-sharing-your-data](https://privacyinternational.org/long-read/3196/no-bodys-business-mine-how-menstruations-apps-are-sharing-your-data) (2019).
- [36] Hill Kulu, Tina Hannemann, Ariane Pailhé, Karel Neels, Sandra Krapf, Amparo González-Ferrer, and Gunnar Andersson. 2017. Fertility by birth order among the descendants of immigrants in selected European countries. *Population and Development Review* (2017), 31–60.
- [37] Adi Kuntsman, Esperanza Miyake, and Sam Martin. 2019. Re-thinking Digital Health: Data, Appisation and the (im)possibility of ‘Opting out’. *Digital Health* 5 (2019), 1–16. <https://doi.org/10.1177/2055207619880671>
- [38] Karen E. Levy. 2015. Intimate Surveillance. *Idaho Law Review* 51, 679–693. <https://doi.org/10.1080/13691058.2014.920528> PMID: 24917459.
- [39] Martina Lindorfer, Matthias Neugschwandtner, and Christian Platzer. 2015. Marvin: Efficient and comprehensive mobile app classification through static and dynamic analysis. In *2015 IEEE 39th annual computer software and applications conference*, Vol. 2. IEEE, 422–433.
- [40] Michele Loi and Markus Christen. 2019. Two Concepts of Group Privacy. *Philosophy & Technology* (2019), 1–18.
- [41] Deborah Lupton. 2014. Self-Tracking Modes: Reflexive Self-Monitoring and Data Practices. *SSRN* (2014). <https://doi.org/10.2139/ssrn.2483549>
- [42] Deborah Lupton. 2015. ‘Mastering Your Fertility’: The Digitised Reproductive Citizen. *Negotiating Digital Citizenship: Control, Contest and Culture* (2015). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2679402
- [43] Deborah Lupton and Sarah Pedersen. 2016. An Australian survey of women’s use of pregnancy and parenting apps. *Women and Birth* 29 (2016), 368–375. <https://doi.org/10.1016/j.wombi.2016.01.008>
- [44] Catriona Ida Macleod. 2019. Expanding reproductive justice through a supportability reparative justice framework: the case of abortion in South Africa. *Culture, Health & Sexuality* 21, 1 (May 2019), 46–62. <https://doi.org/10.1080/13691058.2018.1447687>
- [45] E. Maeda, F. Nakamura, Y. Kobayashi, J. Boivin, H. Sugimori, K. Murata, and H. Saito. 2016. Effects of fertility education on knowledge, desires and anxiety among the reproductive-aged population: findings from a randomized controlled trial. *Human Reproduction* 31, 9 (2016), 2051–2060. <https://doi.org/10.1093/humrep/dew133>
- [46] Maryam Mehrnezhad. 2020. A Cross-Platform Evaluation of Privacy Notices and Tracking Practices. In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, 97–106.
- [47] Maryam Mehrnezhad and Ehsan Toreini. 2019. What Is This Sensor and Does This App Need Access to It? *Informatics Special Issue Human Factors in Security and Privacy in IoT (HFSP-IoT)* (2019). <https://doi.org/10.3390/informatics6010007>
- [48] Amber Milne. 2020. EXPLAINER-How to control women’s sexual health with tech. *Reuters Healthcare* (April 2020). <https://in.reuters.com/article/britain-women-data/explainer-how-to-control-womens-sexual-health-with->

tech-idUSL5N2CB5WS

- [49] Janet Morrissey. 2018. Women Struggling to Get Pregnant Turn to Fertility Apps. (2018). <https://www.nytimes.com/2018/08/27/business/women-fertility-apps-pregnancy.html>
- [50] US Department of Health and Human Services. Accessed 2020. The HIPAA Privacy Rule. <https://www.hhs.gov/hipaa/for-professionals/privacy/index.html> (Accessed 2020).
- [51] Population Division of the Department of Economic and Social Affairs. 2019. 2019 Revision of World Population Prospects. 452 (2019). <https://population.un.org/wpp/>
- [52] Official Journal of the European Union. 2020. Article 4(15) and Recital 35. eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN visited Sep 2020. (2020).
- [53] Isabelle Oomen and Ronald Leenes. 2008. Privacy risk perceptions and privacy protection strategies. In *Policies and research in identity management*. Springer, 121–138.
- [54] World Health Organization. 2020. Sexual and reproductive health: Infertility. *World Health Organization* (2020). <https://www.who.int/reproductivehealth/topics/infertility/keyissues/en/>
- [55] Yong Jin Park. 2015. Do men and women differ in privacy? Gendered privacy and (in) equality in the Internet. *Computers in Human Behavior* 50 (2015), 252–258.
- [56] Dilisha Patel, Ann Blandford, Mark Warner, Jill Shawe, and Judith Stephenson. 2019. “I Feel like Only Half a Man”: Online Forums as a Resource for Finding a “New Normal” for Men Experiencing Fertility Issues. *Proc. ACM Hum.-Comput. Interact.* 3, CSCW, Article 82 (Nov. 2019), 20 pages. <https://doi.org/10.1145/3359184>
- [57] Emmanuel Pernot-Leplay. 2020. China’s Approach on Data Privacy Law: A Third Way Between the US and the EU? *Penn State Journal of Law & International Affairs* 8, 1 (2020).
- [58] Sarah F. Peterson and Wing Kay Fok. 2019. Mobile technology for family planning. *Current Opinion in Obstetrics and Gynecology* 31, 6 (Dec. 2019), 459–463. <https://doi.org/10.1097/GCO.0000000000000578>
- [59] James Pierce, Sarah Fox, Nick Merrill, and Richmond Wong. 2018. Differential Vulnerabilities and a Diversity of Tactics: What Toolkits Teach Us about Cybersecurity. *Proc. ACM Hum.-Comput. Interact.* 2, CSCW, Article 139 (Nov. 2018), 24 pages. <https://doi.org/10.1145/3274408>
- [60] Abbas Razaghpanah, Narseo Vallina-Rodriguez, Srikanth Sundaresan, Christian Kreibich, Phillipa Gill, Mark Allman, and Vern Paxson. 2015. Haystack: In situ mobile traffic analysis in user space. *arXiv preprint arXiv:1510.01419* (2015).
- [61] Tonya Riley. 2020. A popular fertility app shared data without user consent, researchers say. *The Washington Post* (2020). <https://www.washingtonpost.com/technology/2020/08/20/popular-fertility-app-shared-data-without-user-consent-researchers-say/>
- [62] Vanessa Rizk and Dalia Othman. 2016. Quantifying Fertility and Reproduction through Mobile Apps: A Critical Overview. *Arrow for change* 22, 1 (2016), 13–21.
- [63] John Rooksby, Mattias Rost, Alistair Morrison, and Matthew Chalmers. 2014. Personal Tracking as Lived Informatics. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Toronto, Ontario, Canada) (CHI ’14). Association for Computing Machinery, New York, NY, USA, 1163–1172. <https://doi.org/10.1145/2556288.2557039>
- [64] Celia Rosas. 2019. The Future is Femtech: Privacy and Data Security Issues Surrounding Femtech Applications. *Hastings Business Law Journal* 15, 2 (2019). https://repository.uchastings.edu/hastings_business_law_journal/vol15/iss2/5
- [65] Loretta Ross and Rickie Solinger. 2017. Reproductive Justice: An Introduction. (March 2017).
- [66] Hanna Schneider, Julia Wayrauther, Mariam Hassib, and Andreas Butz. 2019. Communicating Uncertainty in Fertility Prognosis. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (Glasgow, Scotland Uk) (CHI ’19). Association for Computing Machinery, New York, NY, USA, 1–11. <https://doi.org/10.1145/3290605.3300391>
- [67] Rakesh Sharma, Kelly R Biedenharn, Jennifer M Fedor, and Ashok Agarwal. 2013. Lifestyle factors and reproductive health: taking control of your fertility. *Reprod Biol Endocrinol.* 11, 66 (2013). <https://doi.org/10.1186/1477-7827-11-66>
- [68] Laura Shipp and Jorge Blasco. 2020. How private is your period?: A systematic analysis of menstrual app privacy policies. *Proceedings on Privacy Enhancing Technologies* 4 (2020), 491–510.
- [69] Elizabeth A. Sternke and Kathleen Abrahamson. 2014. Perceptions of Women with Infertility on Stigma and Disability. *Sexuality and Disability* 33, 3 (2014). <https://doi.org/10.1007/s11195-014-9348-6>
- [70] Frost & Sullivan. 2018. Femtech—Time for a Digital Revolution in the Women’s Health Market. (2018). <https://www2.frost.com/frost-perspectives/femtechtime-digital-revolution-womens-health-market/>
- [71] Didi Surian, Suranga Seneviratne, Aruna Seneviratne, and Sanjay Chawla. 2017. App miscategorization detection: A case study on google play. *IEEE Transactions on Knowledge and Data Engineering* 29, 8 (2017), 1591–1604.
- [72] Sara Suárez-Gonzalo. June 2019. Personal data are political. A feminist view on privacy and big data. *Recerca, Revista de Pensament i Anàlisi* 24, 2 (June 2019), 173–192. <https://doi.org/10.6035/Recerca.2019.24.2.9>
- [73] Kerry van der Berch. 2010. Courts’ struggle with infertility: the impact of hall v. Nalco on infertility-related employment discrimination. *University of Colorado Law Review* 81, 2 (2010), 545–578.
- [74] Paul Voigt and Axel Von dem Bussche. 2017. The eu general data protection regulation (gdpr). *A Practical Guide, 1st Ed.*, Cham: Springer International Publishing (2017).

- [75] Charlie Warzel. 2019. The Loophole That Turns Your Apps Into Spies. *NYT at nytimes.com/2019/09/24/opinion/facebook-google-apps-data.html* (2019).
- [76] Gabriela Weigel, Laurie Sobel, and Alina Salganicoff. 2020. Criminalizing Pregnancy Loss and Jeopardizing Care: The Unintended Consequences of Abortion Restrictions and Fetal Harm Legislation. *Women's Health Issues* 30, 3 (2020), 143-146. <https://doi.org/10.1016/j.whi.2020.03.005>

A LIST OF APPS

No.	App name	Company	Category	No of installs
1	Ovia Fertility: Ovulation & Cycle Tracker	Ovia Health	Medical	1M+
2	Ovulation Calendar & Fertility	Leap Fitness Group	Health & Fitness	1M+
3	Fertility Friend Ovulation App	Tamtris Web Services Inc.	Health & Fitness	1M+
4	Femometer - Fertility Tracker	Bangtang Network Technology Co., Ltd	Health & Fitness	100K+
5	Glow Fertility - Ovulation Tracker, Period Tracker	Glow Inc	Health & Fitness	1M+
6	Period Tracker, Ovulation Calendar & Fertility app	Leap Fitness Group	Health & Fitness	10M+
7	Flo Period tracker, Ovulation & Pregnancy tracker	Flo Health, Inc.	Health & Fitness	50M+
8	Ovulation Calculator & Calendar to Track Fertility	EclixTech	Medical	0.5M+
9	Kindara Fertility & Ovulation Tracker	Kindara, Inc.	Medical	100K+
10	Period Tracker - Period Calendar Ovulation Tracker	Simple Design Ltd.	Health & Fitness	100M+
11	Fertility Diet Guide - Getting Pregnant Faster	Doctor Apps	Health & Fitness	10K+
12	Evoke Fertility Meditations	Auspicious Apps	Health & Fitness	1K+
13	OvuView: Ovulation & Fertility	Sleekbit	Health & Fitness	1M+
14	Ovulation Calculator Fertility	Ovulation Calculator Pty Ltd	Medical	100K+
15	Maya - Period, Fertility, Ovulation & Pregnancy	Plackal Tech	Health & Fitness	5M+
16	Ovulation, Fertility & Pregnancy Tracker Calendar	ElaWoman - Period Tracker & Ovulation Calendar App	Health & Fitness	0.5M+
17	OvTracker - Ovulation & Fertility Tracker	Inidam Leader	Health & Fitness	100K+
18	Ovulation Tracker by Premom: Easily Get Pregnant	premom.com	Health & Fitness	0.5M+
19	My Fertility Charts	Clocking Edge, LLC	Health & Fitness	100K+
20	Fertility Astrology	Fertility Astrology	Communication	500+
21	Ava fertility tracker	Ava AG	Health & Fitness	50K+
22	OvaGraph - Official TCOYF App	Fairhaven Health	Health & Fitness	50K+
23	WOOM - Ovulation & Fertility	Woom Fertility S.L.	Health & Fitness	1M+
24	Fertility Test Analyzer App: Ovulation & Pregnancy	Colnix Technology	Health & Fitness	100K+
25	My Fertility Companion	OB Science S.r.l.	Medical	10K+
26	Ovulation-Fertility Tracker Eveline Cycle Calendar	iXensor Co. Ltd.	Health & Fitness	10K+
27	Trak: Sperm Health & Fertility	Trak Fertility	Health & Fitness	50K+
28	Fertility Diet Guide	Prestige Worldwide Apps, Inc	Health & Fitness	10K+
29	Pearl Fertility	Colorimetrix Inc.	Health & Fitness	1K+
30	Mira Fertility & Ovulation Tracker	Quanovate Tech Inc	Health & Fitness	5K+