Vision: Too Little too Late? Do the Risks of FemTech already Outweigh the Benefits?

MARYAM MEHRNEZHAD*, Royal Holloway, University of London, Egham, UK
LAURA SHIPP, Royal Holloway, University of London, Egham, UK
TERESA ALMEIDA, ITI/LARSyS, Instituto Superior Técnico - U. Lisbon, Portugal
EHSAN TOREINI, Durham University, Durham, UK

Abstract: Female-oriented technologies (FemTech) promise to enable women to take control of their bodies and lives, helping them overcome the many existing challenges in medical care and research. From lack of data about women in general, to bias and discrimination in health studies, data sets, and algorithms, FemTech has come a long way to centre women in the design and development of such systems. Yet, the FemTech industry remains largely unregulated, particularly when it comes to security, privacy, and safety. These issues can lead to catastrophe given the highly sensitive nature of the data FemTech technologies handle. In this paper, we show how such threats are already putting women at risk; where in some cases, the lack of proper security and privacy safeguards can put human life at risk. We also present the results of some of our ongoing research on the massive data collection of FemTech about end-users and others (baby, partner, family, etc.). We set an agenda for research on the security and privacy of FemTech and call for a better legal framework to regulate FemTech.

Additional Key Words and Phrases: FemTech, Cybersecurity, Privacy, Data Protection Laws

ACM Reference Format:
Maryam Mehrnezhad, Laura Shipp, Teresa Almeida, and Ehsan Toreini. 2022. Vision: Too Little too Late? Do the Risks of FemTech already Outweigh the Benefits?. In *2022 European Symposium on Usable Security (EuroUSEC 2022), September 29–30, 2022, Karlsruhe, Germany.* ACM, New York, NY, USA, 10 pages. https://doi.org/10.1145/3549015.3554204

1 INTRODUCTION

This vision paper critically discusses the cybersecurity and privacy of FemTech, with a focus on consumer devices. FemTech includes mobile apps, Internet of Things (IoT) devices and a variety of products and services, that all aim to help women manage their health[1]. They cater to a range of specific health issues (menstruation, menopause, and pregnancy), general wellbeing or longevity (mental health, healthy living), or the management of specific health conditions (breast cancer, migraines, endometriosis). The FemTech market is increasingly growing, and saw a huge boost from the shifts in health management brought about by the pandemic. There are already over 1300 FemTech companies offering a huge range of products, with a market size of $40.2 billion in 2020 alone [10]. Evidence has shown that gender bias has long existed in medical practice, research and education with generalised guidelines created from the study of one gender getting applied to

[*] This work was conducted when the the first two authors were at Newcastle University, UK.

[1] Within this paper, we discuss the users of technologies as women as this falls in line with the how the majority of the industry talks about its users. We do, however, acknowledge and respect that many of these issues face people beyond those who identify as women, and may not affect some women at all.

EuroUSEC 2022, September 29–30, 2022, Karlsruhe, Germany
© 2022 Copyright held by the owner/author(s).
ACM ISBN 978-1-4503-9700-1/22/09.
https://doi.org/10.1145/3549015.3554204

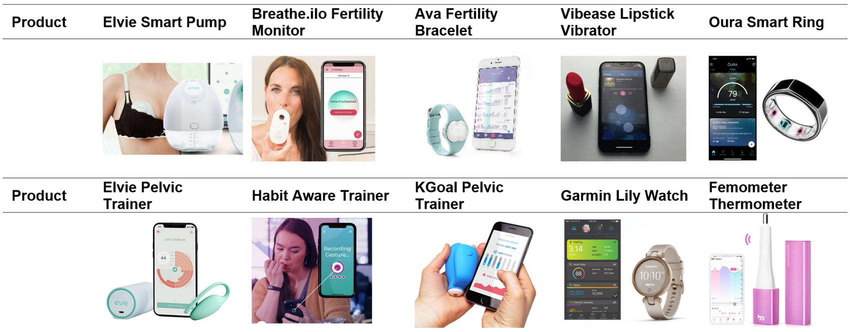

Fig. 1. Examples of FemTech IoT devices. These devices were tested in this pilot study. Figures are taken from the official websites of the products and altered for presentation in the paper.

all. This has implications for women's treatment and health outcomes [16]. Recent publications, such as the book *Invisible Women* [32], have highlighted this problem and brought it into wider public consciousness. Similarly, technology companies have often failed to develop solutions for issues that are faced by many women, like menstrual health. This is best demonstrated by the range of 'comprehensive' health trackers available, which largely failed to originally include a period tracking function, such as the Apple HealthKit.

FemTech has arisen to provide a technological solution to the medical and technological neglect of women's health. FemTech products often work by gaining user-entered data and/or using sensors to take body or environmental measurements (e.g. ovulation detection, basal body temperature). These devices continue to collect data about people's reproductive choices, sexual activities and detailed insights into their lives. By collecting a vast amount of data and processing them through advanced algorithms e.g. AI, these technologies assist in managing varied aspects of people's health. In doing so, they also create large data sets about their users, often around sensitive areas that are not collected by other kinds of technology. There is a lack of clarity in both law and industry practice in terms of how this extremely sensitive data is handled. For example, in relation to how the user is informed and gives consent, third-party sharing, and how algorithmic bias could harm users [6, 27, 38, 42]. The increasingly popular FemTech IoT devices introduce a new set of risks. Various forms of sensors are equipped in FemTech devices and apps including communicational (WiFi, Bluetooth, NFC), biometric (fingerprint, face/voice recognition, etc.), motion, ambient, and other health and medical sensors, the combination of which has not been seen before.

In this paper, we contribute to the body of knowledge by identifying the threat actors and showing how various forms of such threats are already putting women at risk. We also present the results of some of our ongoing research on the massive data collection of FemTech and tracking practices. We set an agenda for research in the security and privacy of FemTech and call for a legal framework to regulate FemTech data.

2 FEMTECH RISKS

Collecting and sharing user data is neither a new, nor a simple problem to tackle; particularly when different demographics e.g., gender is factored in [18, 28]. FemTech privacy, however, can be looked at from various angles including user privacy, inverse privacy [22] (where somebody has your personal data but you do not), differential vulnerabilities [27] (which focuses on the intersectional qualities of individuals and communities), unraveling privacy [31] (where peer pressure causes people to disclose information to avoid the negative inferences of staying silent) and collective privacy (i.e, the privacy of others e.g., child, partner, family, friend). In this section, we contribute to the discussions around FemTech privacy and security by reviewing the literature, identifying the core threat actors and examples of their data misuse.

2.1 (Ex-)Partner and Family

Many of the FemTech solutions e.g., sex toys and fertility apps provide an option for partners to participate in the experience and/or track their partner's sexual and reproductive health input to the system. In some cases, access to partner's intimate data forcefully or without consent is a way of maintaining control. Reportedly, intimate partner violence (IPV), gender-based violence (GBV) and domestic violence have been shown to have significant associations with individuals and couples suffering from infertility, for example, where there is external pressure to become pregnant [8, 27]. Cyberstalking [41] is another serious issue, which could be enabled by the extra tracking functionality of FemTech. Examples of stalkerware usage in intimate partner abuse are well illustrated in [17]; and the use of FemTech in such cases has yet to be documented in literature.

2.2 Employer and Colleagues

FemTech solutions have already found their way to organisational usage [22]. Veliz discusses many examples of misuse of health data in the workplace [44]. Such data can be easily collected by the employer e.g., via offering free health wristbands to employees or under general organisational health plans. There are concerns around how workplace monitoring threatens women's equity [15]. Pregnancy redundancies and impact on promotions have been and still are a reality and are a big source of anxiety for many working women in almost all countries including the UK [6]. Access and use of FemTech data when making employment-related decisions is generally an unknown and unregulated process. Similarly, discrimination in the workplace due to infertility is an ongoing issue [43]. In her recent papers [14, 15], Brown discusses the potential consequences of data collection through FemTech; suggesting that these tools could end up increasing the risks of sex discrimination and sexual harassment in the workplace. Given that FemTech solutions (e.g, fertility apps) are already sharing these data with third parties including employers [24, 36] without user consent [27], these technologies could be used to further gender inequality at work.

2.3 Insurance Firms

Health insurance discrimination on the basis of health status is becoming a pressing issue [20, 35]. The progressive market of personalised medicines and health insurance is continuing to make such discrimination even more serious and complex. Scatterday argues that without users' knowledge, their FemTech data is used to "train algorithms used in hiring, housing, insurance, and other crucial decisions"[36]. Such trained systems may then make harmful predictions, such as increased insurance costs due to perceived infertility. Health insurance is always entwined with "unraveling privacy" where people might have to share their health and medical background to avoid the negative impact on their insurance packages. Health insurance can also explicitly show how the "privacy of others" could be violated. Consider the case of a person whom an insurance company has obtained access to the health data of their parents, siblings and other relatives. If a possibility of a pre-existing medical condition (e.g., infertility or breast cancer) is identified, such insurance firms will not support the person or do it at much higher rates. A situation that might continue even after the death of the users; impacting their offspring.

2.4 Cyber-criminals

FemTech data can be of particular interest to cyber-criminals. FemTech data deals with a complex mix of health, medical, biometric, and genetic data, alongside sexual activities/orientation, reproductive decisions, and even religious and political views [27]. Criminals could use such data to blackmail or harm, particularly when taking socio-cultural differences into account; more marginalised groups will have more to lose from such disclosures. There have already been cases of this within health tech. In 2017, criminals obtained access to medical reports of a clinic and blackmailed its patients [44]. The attackers published thousands of private photos, passport scans, and other personal data. Data breaches in FemTech is even more serious because of the sensitive nature of the data [34]. Since the entire sector is not properly regulated, there are more risks of more serious attacks on a wider range of platforms (e.g, PC programs, mobile apps, IoT devices) and beyond.

2.5 Advertising Companies

While tracking for personalised advertising is present in almost all mobile apps, FemTech deals with a complex and sensitive combination of data. This means the tracking of users enabled by such data may cause more significant impacts on a person's life. From app-only data collection to sensor-enabled FemTech devices, with extra processing via advanced algorithms e.g., AI, FemTech data reveal people better than they know themselves – inverse privacy. FemTech data also concerns collective privacy [25] (privacy of others). This includes their contacts, connections and relations, and the privacy of co-constructed personal information. Reportedly, these apps 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 [7]. Apart from the academic research on FemTech tracking practices such as [27, 38], this fact has been documented in several news reports in the last few years [29], including the case of selling FemTech data by data marketplaces [19].

2.6 Political and Religious Organisations

FemTech apps commonly include health-based discussion forums via builtin features and social media plugins. This information is often seen by companies and third parties as 'public' whereas users may consider these forums as closed spaces [38]. The interests on the groups behind the apps are not always clear to the user. For example in 2019, a Guardian investigation has found a period and fertility tracker app was funded by anti-abortion, anti-gay Catholic campaigners and where it was unclear how the aggregated data sets were generated and used by the app and beyond it [23]. Moreover, the potential for new opportunities for misinformation to spread through such forums remains high, a phenomenon well-documented on other healthcare issues e.g., anti-vaccination movements [30]. It could be particularly dangerous in cases where organisations are pushing certain messages in line with their agendas often obscured from the end-user.

2.7 Governments

FemTech data can be particularly of interest of governments. The recent debates around the overturn of the abortion law in the US Supreme Court [29] has shown very well how FemTech (e.g., apps) can enable such a systematic tracking and controlling of women's bodies. Evidently, such concerns are very real, e.g., the case of an ovulation-tracking app which allowed anyone to access all the user's health data [13]. Different governments might want to obtain such data for different purposes. An example is tracking the menstrual cycles of migrant girls in the USA [12] through two fallacious apps with an agenda based on religious beliefs or in line with discriminatory government policies dictating who can and cannot get pregnant [39]. Another example is the news around the tracking of Iranian women's pregnancies (e.g., via registering every lab pregnancy test in a centralised system) to prevent abortion, and considering legal consequences for an unlawful abortion [11]. Each of these demonstrate a deep violation of the human rights to privacy and bodily autonomy.

2.8 Medical and Research Companies

In 2019, data about millions of patients in the UK's National Health Service (NHS) was sold to US-based and other international pharmaceutical companies for research purposes without prior notice or consent [44]. While this practice was not new and has been done in the past (e.g., sharing with Google) [33], it created a number of privacy concerns. Even if such data sharing is performed by applying some form of privacy-preserving mechanisms, the current protection is not enough in light of emerging technologies. Previous research on medical records has shown that around 90% of Americans could be identified with three types of data: birth date, gender, and zip code [40]. During the pandemic sharing medical and health data became a common practice. As Veliz demonstrates in [44], during crises, decisions are taken opportunistically. By using the appeal of "saving lives", even the slightest resistance to a proposed extreme measure is silenced. It is essential to note that privacy losses kill too, e.g., the suicide of a Spanish mother following imaged-based sexual abuse [44]. FemTech data –similar to any other health and medical data–is often for sale. This problem intensifies when we learn, as highlighted in this paper, how multiple parties are indeed interested in such data.

The promise of developing FemTech is to empower women and improve women's health and quality of life, but in practice, and as we have elucidated in this section, the risks are already outweighing the benefits.

3 PILOT EXPERIMENTS AND RESULTS

This section outlines the preliminary study we have conducted into the privacy and security of FemTech IoT devices currently available for purchase in the UK. These devices were selected by reviewing lists of companies on FemTech community pages, filtering the companies whose offerings included devices. This was then sifted again to those that made 'smart' devices, that were already on the UK market. We examined a subsection of the devices in order to determine the appropriateness of the tests for these types of devices. We studied the devices from different angles including the data collection, security features, and privacy practices of IoT devices and Apps. Here, we show how a sample set of FemTech IoT devices collect a wide range of data about the user, their body, others, environment, and beyond. We also present the results of our studies on how the websites of these IoT devices track users.

3.1 FemTech Devices and Data Types

In Fig. 1, we have identified off-the-shelf products in the UK, with a range of functionalities and sensors. For example, some devices fell under the category of fertility (Ava, Breathe.ilo and Femometer), yet had different ways of measuring the fertile window (sleep, temperature, CO2). We set these devices up (turning on and connecting to the Android app), and worked with them as an end-user. We examined what types of data these devices collect, as presented in Table 1. These devices collect a wide range of data including user-entered data and sensor-collected data. Such **user data** include, but are not limited to: information about User (e.g., name, photo, age, gender), Contact (e.g, mobile, email, address), Lifestyle (e.g., weight, diet, sleep), Period (e.g., cycle length, ovulation days), Pregnancy (e.g., test results, due dates, IVF), Nursing (e.g., type, volume, pain), Reproductive organs (e.g., cervical mucus, muscle strength), Sexual activities (e.g., date, contraceptives, orgasm), Medical information (e.g., medication type, blood pressure, lab reports scan), Physical symptoms (e.g., headache, constipation), and Emotional symptoms (e.g., happy, anxious). In addition to data directly concerning the user, these devices also ask for or automatically

Table 1. User data collected by FemTech IoT devices

Product	Elvie Smart Pump	Breathe.ilo Fertility Monitor	Ava Fertility Bracelet	Vibease Lipstick Vibrator	Oura Smart Ring	Elvie Pelvic Trainer	Habit Aware Trainer	KGoal Pelvic Trainer	Garmin Lily Watch	Femo-meter Themom.
User's data, sym = symptoms										
User info	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Contact info	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Lifestyle		✓	✓		✓	✓	✓	✓	✓	✓
Period		✓	✓		✓				✓	✓
Pregnancy		✓	✓							✓
Nursing	✓									
Repro. organs		✓	✓			✓		✓	✓	✓
Sex activities		✓	✓	✓					✓	✓
Medical			✓		✓				✓	✓
Physical sym		✓	✓				✓		✓	✓
Emotional sym		✓	✓						✓	✓
Others' data										
Partner info				✓						✓
Social media				✓					✓	✓
Child info	✓					✓	✓			✓
IoT/Mobile device's resources										
Storage		✓		✓	✓		✓		✓	✓
Call/Contacts				✓					✓	
Calendar									✓	
WiFi	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Cam/Mic				✓	✓		✓		✓	✓
GPS	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Bluetooth	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Sensor data	✓	✓	✓		✓	✓	✓	✓	✓	✓
AI-enabled		✓	✓		✓					

collect **data about others** including: Baby or child (e.g., nursing, sleep cycles, fetal movements), Social media profiles, forums, or plugins (e.g., Facebook, Spotify), Partner (e.g., details of partnered sex activities, name, age, photo). These technologies might even ask a bout the medical history of the user's family. Finally, These systems also have access to the **devices' resources** on the phone and the IoT device e.g, camera, microphone, device files and storage, phone's contacts and calls, communicational sensors (WiFi, Bluetooth, NFC), motion and environmental sensors from the phone or the device (e.g., temperature, pressure, Co2).

The amount of data collected by each device and app varied across these IoT devices. For example, the Garmin Lily app had the most calls of the mobile device's resources, requesting all possible permissions alongside information about a user's menstrual cycle, sex life and lifestyle. Within the Femometer Vinca II Themometer app, you could provide details of miscarriages, expected term of pregnancy, use of assisted reproductive technology, alongside a variety of measurements of the fetus. You can even upload lab test results through the camera function. Comparatively, the Elvie Pump and Pelvic Floor Trainer collected the least amount of data and only requested permissions related to Bluetooth (including the use of location access as required with Android OS) and WiFi.

3.2 Tracking Practices of the Websites

In order to highlight the non-compliant practices of these systems, we continued our experiments by testing the websites of these products for their tracking practices. We opened these websites on Chrome on a Mac laptop in order to observe (i) the presence of a cookie (privacy) notice, and (ii) its user control options. We then used Brave (a privacy-oriented browser) to identify how many trackers are activated when the website is loaded for the first time, and before any engagement with the cookie notice. Brave uses a block-by-design mechanism that blocks and reports ads and

Table 2. Tracking practices of the websites of the FemTech IoT devices

Product	no. of Trackers (before user engagement)	Cookie Dialogue's Control Options	Opt out Option
Elivie Smart Pump	9	Accept all/Customize	N/A
Breathe.ilo Fertility Monitor	7	Accept	N/A
Ava Fertility Bracelet	7	Accept all/Cookies Settings	N/A
Vibease Lipstick Vibrator	2	N/A	N/A
Oura Ring Generation 3	5	N/A	N/A
Elvie Pelvic Floor Trainer	9	Accept all/Customize	N/A
HabitAware Keen2 Bracelet	12	N/A	N/A
kGoal Pelvic Floor Trainer	24	N/A	N/A
Garmin Lily Watch	2	Accept/Decline/Manage Settings	Yes
Femometer Vinca II Thermometer	2	Got it	N/A

website trackers while the webpage is getting parsed [2]. Our results show that all of these websites implemented some form of tracking. As shown in Table 2, 7 out of 10 planted at least 5 tracker cookies in the user's browser (user tracking, marketing and analysis cookies mainly for user profiling purposes), 2 even more than 10 trackers. Moreover, the webpage visitors are given limited control options. 6 out of 10 websites did not present any options to users to customize the cookie settings, and 4 did not present any cookie notice at all. These are only a subset of the non-compliant practices, when using the GDPR framework [26], which are present in these products' ecosystems. We plan to complete this research by studying more devices and performing a comprehensive security and privacy analysis on devices, apps, and websites, alongside user studies.

4 RESEARCH CHALLENGES AND OPPORTUNITIES

In this section we discuss the areas that need the attention of the research community as well as the industry and the regulatory bodies.

4.1 Regulations

Although a wide range of regulations may concern the data types collected by FemTech, the sector is yet to be properly regulated. Such regulations include the California Consumer Privacy Act (CCPA)[21], Health Insurance Portability and Accountability Act (HIPPA) [5], Federal Food, Drug, and Cosmetic Act (FD&C Act) [3], Federal Trade Commission Act [4], the General Data Protection Regulations (GDPR)[45], UK Medicines & Healthcare products Regulatory Agency (MHRA) [1], and the EU Medical Devices [2]. As an example, the GDPR recognises some types of personal data as more sensitive- referred to as "special category data", and gives these data types extra protection [9]. 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, data concerning health, sex life, and sexual orientation. The law strictly limits the processing of special category data, although there are some exceptions. The GDPR exceptions are indeed debatable; another matter which is beyond the scope of this paper. while there is an overlap between FemTech data and some of the GDPR's special categories of data, there is no clear mention of FemTech data in these regulations.

We believe that it is vital to identify the gaps in the existing regulations, as well as studying how FemTech products can violate these related laws and misuse such gaps. An example of this can be seen in FemTech companies, such as KGoal, stating the data around a person's pelvic floor health and workouts will not "... be deemed to be an electronic health record or an electronic medical

[2] Brave.com

record for any purpose whatsoever under any law or regulation, ..." [3]. By stating that this data is not special category, as it is not specifically mentioned within GDPR, the company overcomes the need to protect it. We invite the researchers in academia and industry as well as the policymakers to conduct research on a robust framework to revisit some of the established laws and/or initiate new ones to protect the FemTech users from the existing and potential harms.

4.2 System Studies

A number of system studies have been performed on a subset of FemTech apps e.g., analysis of the data collection practices of the period tracking app ecosystem and their policies [38], measuring the tracking practices of fertility apps and their compliance to the GDPR [27], and a traffic analysis and policy review (with focus on HIPPA [5]) of a subset of iOS apps [22]. Very limited work has gone into the security and privacy assessment of FemTech IoT devices [42]. We argue that IoT devices are putting and will continue to put FemTech users at greater risks due to the following reasons. First, IoT sensors create new opportunities for data collection than just apps and have the potential to compromise the users' security and privacy more significantly. Second, they interact with more aspects of our lives, bodies, and environments than other technologies; meaning their risks may lead to critical safety issues. Third, not only have we demonstrated that the FemTech sector is yet to be regulated, but also the lack of enforceable IoT regulation is already well-known [37]; compounding the issue. In this paper, we identified the threat actors, and we will continue to work on this by also identifying the threat vectors of FemTech IoT. Other future work includes identifying the data collection of FemTech systems, implemented security and privacy enhancing technologies (PETs), existing vulnerabilities, and potential security measures to mitigate them.

4.3 User Studies

To the best of our knowledge, there are no dedicated user studies on the privacy and security of FemTech IoT devices. It is imperative to understand how users and those whose privacy may also be implicated in these technologies (partners, family members, etc.) relate to these technologies, and how well they are informed of its risks. Such user studies can reflect various forms of privacy (collective, unraveling, inverse, etc.). We would like to find out how the risks of data usage from FemTech IoT devices will be felt differently, as some people may have more to lose from its exposure. Moreover, the results of such studies, can contribute to a robust framework offering privacy, user-centred and security-by-design for the next generation of FemTech products, ensuring that marginalised and vulnerable users are well-protected. Designing risky scenarios for such user studies can be followed by borrowing the 'differential vulnerabilities' lens introduced in the context of fertility technologies in [27]. The three dimensions of differential vulnerabilities are: the exposure to the hazard, the effect of any exposure, and the capacity of response for the user. These dimensions would help the researchers to conduct inclusive studies and compare the results.

5 CONCLUSION

This vision paper elucidates the many threat actors that could put FemTech IoT users at risk of mismanagement, misuse and misappropriation of their sensitive data. As the industry expands, so too do its risks, and it is imperative for research on the legal, technological and human dimensions of this issue to continue. We show that despite the popularity of FemTech products, their risks are largely outweighing their benefits, unless more can be done to protect user security and privacy. We bring these issues to attention and urgently call for further research on them to be conducted.

[3] www.kgoal.com/pages/privacy-policy

ACKNOWLEDGMENTS

This work has been supported by the PETRAS National Centre of Excellence for IoT Systems Cybersecurity, which has been funded by the UK EPSRC under grant number EP/S035362/1.

REFERENCES

[1] Medicines & healthcare products regulatory agency. https://www.gov.uk/government/organisations/medicines-and-healthcare-products-regulatory-agency.

[2] Medical devices. *European Commission*, 2017. https://ec.europa.eu/growth/single-market/european-standards/harmonised-standards/medical-devices_en.

[3] Federal food, drug, and cosmetic act (fd&c act), amendments act of 2008, 2018. https://www.fda.gov/regulatory-information/laws-enforced-fda/federal-food-drug-and-cosmetic-act-fdc-act.

[4] Federal trade commission act. *Independent agency of the United States government*, 2018. https://www.ftc.gov/legal-library/browse/statutes/federal-trade-commission-act.

[5] Health insurance portability and accountability act of 1996 (hipaa), 2018. https://www.cdc.gov/phlp/publications/topic/hipaa.html.

[6] Discrimination during maternity leave and on return to work. *Maternity Action*, 2019. https://maternityaction.org.uk/advice/discrimination-during-maternity-leave-and-on-return-to-work/.

[7] How menstruation apps are sharing your data. *Privacy International*, 2019. https://privacyinternational.org/long-read/3196/no-bodys-business-mine-how-menstruations-apps-are-sharing-your-data.

[8] Sexual and reproductive health: Infertility. *World Health Organization*, 2020. https://www.who.int/reproductivehealth/topics/infertility/keyissues/en/.

[9] What is special category data? *ICO*, 2020. 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/.

[10] Femtech industry in interactive charts. 2021. https://www.femtech.health/interactive-chartsh.

[11] Iran death penalty threat for abortion unlawful: Un rights experts. *United Nations*, 2021. https://news.un.org/en/story/2021/11/1105922.

[12] P. Alvarez. 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.

[13] J. Beilinson. Glow pregnancy app exposed women to privacy threats. 2016. Consumer Reports at consumerreports.org/mobile-security-software/glow-pregnancy-app-exposed-women-to-privacy-threats.

[14] E. Brown. Supercharged sexism: The triple threat of workplace monitoring for women. *SSRN 3680861*, 2020.

[15] E. Brown. The femtech paradox: How workplace monitoring threatens women's equity. *Jurimetrics*, 2021.

[16] D. Centola, D. Guilbeault, U. Sarkar, E. Khoong, and J. Zhang. The reduction of race and gender bias in clinical treatment recommendations using clinician peer networks in an experimental setting. *Nature communications*, 12(1):1–10, 2021.

[17] S. Chan. Hidden but deadly: Stalkerware usage in intimate partner stalking. *Introduction To Cyber Forensic Psychology: Understanding The Mind Of The Cyber Deviant Perpetrators*, pages 45–66, 2021.

[18] K. Coopamootoo, M. Mehrnezhad, and E. Toreini. " i feel invaded, annoyed, anxious and i may protect myself": Individuals' feelings about online tracking and their protective behaviour across gender and country. *USENIX*, 2022.

[19] J. Cox. Data marketplace selling info about who uses period tracking apps, 2022. https://www.vice.com/en/article/v7d9zd/data-marketplace-selling-clue-period-tracking-data .

[20] M. Crossley. Discrimination against the unhealthy in health insurance. *U. Kan. L. Rev.*, 54:73, 2005.

[21] L. de la Torre. A guide to the california consumer privacy act of 2018. *Available at SSRN 3275571*, 2018.

[22] J. Erickson, J. Y. Yuzon, and T. Bonaci. What you don't expect when you're expecting: Privacy analysis of femtech. *IEEE Transactions on Technology and Society*, 2022.

[23] J. Glenza. 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.

[24] D. Harwell. Is your pregnancy app sharing your intimate data with your boss? *The Washington Post*, 2019. https://www.washingtonpost.com/technology/2019/04/10/tracking-your-pregnancy-an-app-may-be-more-public-than-you-think/.

[25] M. Loi and M. Christen. Two concepts of group privacy. *Philosophy & Technology*, pages 1–18, 2019.

[26] M. Mehrnezhad. A cross-platform evaluation of privacy notices and tracking practices. In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 97–106. IEEE, 2020.

[27] M. Mehrnezhad and T. Almeida. Caring for intimate data in fertility technologies. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, pages 1–11, 2021.

[28] M. Mehrnezhad, K. Coopamootoo, and E. Toreini. How can and would people protect from online tracking? *Proceedings on Privacy Enhancing Technologies*, 1:105–125, 2022.

[29] C. Page. As roe v. wade reversal looms, should you delete your period-tracking app?, 2022. https://techcrunch.com/2022/05/05/roe-wade-privacy-period-tracking.

[30] G. Pennycook and et al. Shifting attention to accuracy can reduce misinformation online. *Nature*, 2021.

[31] S. R. Peppet. Unraveling privacy: The personal prospectus and the threat of a full-disclosure future. *Nw. UL Rev.*, 2011.

[32] C. Perez. Invisible women exposing data bias in a world designed for men, 2020.

[33] J. Powles and H. Hodson. Google deepmind and healthcare in an age of algorithms. *Health and technology*, 2017.

[34] C. Rosas. The future is femtech: Privacy and data security issues surrounding femtech applications. *Hastings Business Law Journal*, 2019.

[35] S. Rosenbaum. Insurance discrimination on the basis of health status: An overview of discrimination practices, federal law, and federal reform options: Executive summary. *Journal of Law, Medicine & Ethics*, 37(S2):101–120, 2009.

[36] A. Scatterday. This is no ovary-action: Femtech apps need stronger regulations to protect data and advance public health goals. *North Carolina Journal of Law & Technology*, 23(3):636, 2022.

[37] B. Schneier. New iot security regulations. *Schneier on Security Blog*, 2018. https://www.schneier.com/blog/archives/2018/11/new_iot_securit.html.

[38] L. Shipp and J. Blasco. How private is your period?: A systematic analysis of menstrual app privacy policies. *Proc. Priv. Enhancing Technol.*, 2020(4):491–510, 2020.

[39] C. Shoichet. In a horrifying history of forced sterilizations, some fear the us is beginning a new chapter, 2020. https://edition.cnn.com/2020/09/16/us/ice-hysterectomy-forced-sterilization-history/index.html.

[40] O. Solon. Data is a fingerprint: why you aren't as anonymous as you think online, 2018. https://www.theguardian.com/world/2018/jul/13/anonymous-browsing-data-medical-records-identity-privacy.

[41] F. Stevens, J. R. Nurse, and B. Arief. Cyber stalking, cyber harassment, and adult mental health: A systematic review. *Cyberpsychology, Behavior, and Social Networking*, 24(6):367–376, 2021.

[42] J. Valente, M. A. Wynn, and A. A. Cardenas. Stealing, spying, and abusing: Consequences of attacks on internet of things devices. *IEEE Security & Privacy*, 17(5):10–21, 2019.

[43] K. van der Berch. Courts' struggle with infertility: the impact of hall v. nalco on infertility-related employment discrimination. *University of Colorado Law Review*, 81(2), 2010.

[44] C. Veliz. Privacy is power: Why and how you should take back control of your data. *Int. Data Privacy Law*, 2022.

[45] P. Voigt and A. Von dem Bussche. The eu general data protection regulation (gdpr). *A Practical Guide, 1st Ed., Cham: Springer International Publishing*, 2017.