Mind the FemTech Gap: Regulation Failings and Exploitative Systems

Maryam Mehrnezhad, Royal Holloway University of London, UK (maryam.mehrnezhad@rhul.ac.uk)
Thyla van der Merwe, formerly at ETH Zurich, Switzerland (tjvdmerwe@gmail.com)
Michael Catt, Newcastle University, UK (michael.catt@newcastle.ac.uk)

Abstract

We study the female-oriented technologies (FemTech) ecosystem including regulations, IoT systems, mobile apps, and websites and reveal the exploitative patterns embedded in such systems due to inadequate regulations and/or enforcement. We advocate for policymakers to explicitly acknowledge and accommodate the risks of these technologies in the relevant regulations.

1 Introduction

Generally known and referred to as female-oriented technologies (aka female technologies or 'FemTech'), FemTech is a term applied to the collection of digital technologies focused on women's health and wellbeing, as the majority of the industry talks about its users. We, however, acknowledge that these products are available for people across all gender identities. FemTech products come in all forms of types and applications, ranging from mobile period apps to fertility-tracking wearables to IVF services on the blockchain. Predicted to be a $75-billion industry by 2025, this sector is booming. Consequently, they also introduce new risks and harms associated with the collection of sensitive health, medical, and sex data that are not identified and addressed in the related regulations.

There is some research addressing the security and privacy (SP) risks that can originate from the mismanagement, misuse, and misappropriation of intimate data on issues such as abortion and (in)fertility (e.g., [8]). However, limited work has gone into exploring the laws, regulations, policies and standards surrounding FemTech's SP risks. The existing work is either mainly around US regulations e.g., [11,12], explores the gaps without demonstrating how such gaps can be exploited (e.g., [6]), focuses on user studies (e.g., [5]), or is limited to a subset of FemTech solutions such as fertility tracker apps [8].

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)[1], Health Insurance Portability and Accountability Act (HIPPA)[2], Federal Food, Drug, and Cosmetic Act (FD&C Act)[3], Federal Trade Commission Act[4], the General Data Protection Regulations (GDPR)[5], the Swiss Federal Act on Data Protection[6], UK Medicines & Healthcare products Regulatory Agency (MHRA)[7], and the EU Medical Devices regulation [8]. Note that there is a range of standards related to FemTech e.g., the ISO 13485 Medical devices[9] and ISO 3533:2021 Sex toys (Design and safety requirements for products in direct contact with genitalia, the anus, or both)[10]. Here we only focus on the related regulations with standardisation beyond the scope of this paper.

We conduct our studies in the UK and Switzerland. These two countries are particularly interesting since they are not EU members. However, they have significant business operating in the EEA which makes them relevant to the EU regulations including the general data protection laws and medical and health ones. Specifically, we aim to answer the following research questions: **RQ1**: What gaps exist in the applicable

USENIX Symposium on Usable Privacy and Security (SOUPS) 2023.
August 6–8, 2023, Anaheim, CA, USA

[1] oag.ca.gov/privacy/ccpa

[2] cdc.gov/phlp/publications/topic/hipaa.html

[3] fda.gov/regulatory-information/laws-enforced-fda/federal-food-drug-and-cosmetic-act-fdc-act

[4] ftc.gov/legal-library/browse/statutes/federal-trade-commission-act

[5] ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

[6] fedlex.admin.ch

[7] gov.uk/government/organisations/medicines-and-healthcare-products-regulatory-agency

[8] ema.europa.eu/en/human-regulatory/overview/medical-devices

[9] iso.org/iso-13485-medical-devices.html

[10] iso.org/standard/79631.html

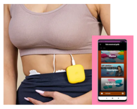
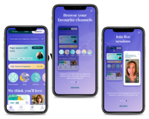
Category	(1) Pregnancy and nursing	(2) Reproductive health and contraception	(3) Fertility and Menstrual health	(4) General health care	(5) Pelvic and uterine health care
Product	Elvie smart pump 	DAYSY cycle computer 	Lady Comp fertility tracker 	HidrateSpark 3 water bottle 	Perifit kegel exerciser
Category	**(6) Sexual health**	**(7) Women's wellness**	**(8) Menopause care and**	**(9) Longevity**	**(10) Mental health**
Product	Frida (Vibio) sex toy 	Livia period pain reliever 	Balance menopause support app 	Daviky pill organiser 	Ivy (Bellabeat) health tracker

Figure 1: Examples of Femtech products (IoT, Apps) and their categories. These categories are based on FemTech Analytics, a strategic analytics agency focused on the FemTech sector (femtech.health).

laws and regulations when it comes to female-related data? **RQ2:** How do FemTech systems (apps, websites, IoT devices) misuse these gaps in the regulations, either intentionally or unintentionally? **RQ3**: How do these systems violate the applicable laws and regulations?

We review the existing regulations related to FemTech in the UK, EU, and Switzerland to identify the gaps. We run experiments on a range of FemTech devices, apps, and websites and identify several exploitative practices. We advocate for policymakers to explicitly acknowledge and accommodate the risks of these technologies in the relevant regulations.

2 Related Work

FemTech products include mobile apps, connected devices and online services covering menstruation, menopause, fertility, pregnancy, nursing, sexual wellness, and reproductive health care, to name a few categories. The SP of FemTech can be investigated by looking into IoT hardware, product websites, mobile apps, cloud datasets, etc. In [10], it is suggested that FemTech privacy should be looked at via different lenses. These include the cases where somebody (e.g., a company) has user personal data but the user does not –inverse privacy [3], when peer pressure causes people to disclose information to avoid the negative inferences of staying silent –unraveling privacy, when the privacy of others (e.g., child, partner, family, friend) also matters –collective privacy [1], and when systems should also focus on the intersectional qualities of individuals and communities –differential vulnerabilities [8]. Multiple FemTech threat actors have been identified in [10]. These interested parties include, but are not limited to: (ex-)partner and family, employers and colleagues, insurance firms, advertising companies, political and religious organisations, governments, and medical and research companies.

Such threat actors may exploit FemTech systems in various ways by performing attacks at different points of the ecosystem e.g., human dimensions, hardware vulnerabilities, dataset attacks, app and website exploits, etc. Examples of such system studies include measuring the tracking practices of FemTech IoT devices [1, 10], fertility apps and their compliance with the GDPR [8], as well as traffic analysis and policy review (with a focus on HIPPA) of a subset of iOS apps [3]. Limited work has gone into the SP assessment of FemTech IoT devices [13]. The SP community is yet to properly investigate the data collection of FemTech ecosystems, (lack of) implemented security and privacy-enhancing technologies (PETs), the existing vulnerabilities, and potential SP measures to mitigate them.

IoT systems interact with more intimate aspects of our lives, bodies, and environments than other technologies; meaning their risks may lead to critical safety issues. We argue that the intersection of health and medical solutions, user general data, and the data produced and collected by IoT devices and apps are putting and will continue to put FemTech users at greater risks, as evident by the ongoing research after the overturning of Roe vs Wade [5].

3 Methodology

The methods we use fall into two groups: reviewing the regulations and conducting system studies.

3.1 Critical Review of Regulations

Various aspects of FemTech data and systems make it challenging to point to one single law for the protection for FemTech data. The data collected by such technologies can be related to regulations around general data protection, work discrimination, software, apps, IoT, medical and health, and

Table 1: List of regulations in EU, UK, and Switzerland related to FemTech systems and data.

Category	Law	Enforcement Year	Country
General	General Data Protection Regulation (GDPR)	2018	EU, UK
General	Swiss Federal Act on Data Protection (FADP)	1993	Switzerland
Health & Medical	MHRA Medical Devices Regulations	2002	UK
Health & Medical	Regulation (EU) 2017/745 for Medical Devices	2021	EU

human rights. We focus on the general data protection laws and those concerning medical and health data. More specifically, we review the General Data Protection Regulations (GDPR), the Swiss Federal Act on Data Protection (FADP), UK Medicines & Healthcare Products Regulatory Agency (MHRA), and the Regulation (EU) 2017/745 for Medical Devices.

For each law, we go through its public documents and manually search for mentions of Fem-Tech data via a few key words. For building this keywords set we use the categories in Fig. 1 and expand on it. Our keywords include, but are not limited to: Fem-Tech, women, period, fertility, pregnancy, abortion, fetus, baby, health, sex, menopause, mental health, reproductive, contraception, nursing, longevity, wellness, pelvic, uterine, breast, milk, female, cycle, birth, hormone, ovulation, lactation, menopause, etc. We identify the (lack of) related sections of each law regarding FemTech.

3.2 System Studies

In Fig. 1, we have identified off-the-shelf products for the different FemTech categories. The products on the market can belong to multiple categories. For instance, a pelvic floor trainer can also be an intimate massager. Some of these products (e.g., pill organiser) would also categorise as general health solutions. Our system study experiments are performed in the UK between September 2022 to April 2023. We purchased these devices in either the UK or Switzerland by searching for FemTech products in each category. Table 2 shows that six of these devices (no.: 1,2,4,5,6,10) are connected to an app, one does not offer an app and is a standalone device (no.: 2), two are not connected to their apps (no.: 7,9), and one is only an app (no.: 8). These devices and apps are manufactured in various countries including UK, USA, Switzerland, Germany, France, Israel, and China and their price varies based on the product (from free apps with in-app purchases to £500-600). We chose this combination for two reasons. First, we wanted to cover a range of products from different brands with various functionalities and features. And second, some of these categories do not offer off-the-shelf IoT devices and are limited to apps or non-IT products only.

Data Collection: We installed all the Android apps associated with these products from the Google Play App Store. In the case of IoT devices, we set them up i.e., charging them, turning them on and connecting them to the Android app. We then started using these devices and their companion apps as an end-user. We observed what type of data each of these devices collect either via the user's manual input (e.g., name and age) or automatic data collection via the device's sensors and other resources e.g., access to phone contacts. These data types are presented in Table 2. For these experiments, we followed the same structure of recent papers [1, 10]. Two of the authors repeated this process for each app independently (on two Google Pixel 6 phones) and logged their observations. If there was an inconsistency in the result, the experiment was repeated jointly for a third time.

Privacy Notice: The ePrivacy Directive[11] ("ePD", aka "cookie law") provides supplementary rules to the GDPR. According to the ePD website, publishers must rely on user consent when collecting and processing personal data using non-mandatory (not strictly necessary for the services requested by the user) cookies or other technologies. This is in accordance with the guidance given by the European Data Protection Board and the ICO. To comply with the GDPR, and according to the ICO guidelines, the online service providers (e.g., product websites and Android apps) are required to inform the users about tracking technologies (e.g., cookies), their purpose and reasons, and obtain the person's consent to use the tracking data. This consent must involve some form of unambiguous positive action (e.g., ticking a box and clicking a link) and be separated from other matters (e.g. terms and conditions 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 users taking positive action before it is set on their device does not represent valid consent and is a violation.

In order to highlight the non-compliant practices of these

[11] eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02002L0058-20091219

devices and systems, we followed the same methods we used in [7, 8] and tested the websites and apps of these products for their tracking practices. For websites, we opened each website on Chrome on a MacBook laptop in order to observe (i) if there is a cookie (privacy) notice, and (ii) what the user control options were. For apps, when we installed each app on an Android device, we opened it for the first time as well as later (a few times), and again to test if there is a cookie (privacy) notice and the control options. In order to review the privacy policies, when there was a link available, we followed the same approach used in the review of the regulations by looking for FemTech-related keywords.

Tracking Practices: To study the tracking behaviour of the websites of these devices, we used Brave[12] (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 website trackers while the webpage is getting parsed. For identifying the app trackers, we use Exodus Privacy app (a privacy audit platform for Android apps)[13] 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.

4 Applicable Laws and Regulations

In this section, we provide the results of our review of the laws and regulations.

4.1 General Data Protection Regulation

Due to Brexit, and since the EU GDPR is an EU regulation and no longer applies to the UK. If a company operates inside the UK, they need to comply with the Data Protection Act 2018 (DPA 2018). According to the ICO, the provisions of the EU GDPR have been incorporated directly into UK law as the UK GDPR. In practice, there is little change to the core data protection principles, rights and obligations.

In the GDPR, personal data is defined as: "information that relates to an identified or identifiable individual". The GDPR recognises some types of personal data as more sensitive, referred to as 'special category data', and gives them extra protection [14]. This data includes 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 GDPR prohibits the processing of special category data. This requirement is on top of all the other subject rights for general personal data.

When we search in the GDPR articles and guidelines, FemTech data categories are not mentioned directly. There is an overlap between FemTech data and some of the special categories of data e.g., health, sex life, sexual orientation, and potentially genetic, biometric data, and even racial or ethnic origin, political opinions, religious or philosophical beliefs. The GDPR defines the following data: *Health data*: "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". *Genetic data*: "means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question". *Biometric data*: "means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data". It does not define data concerning sex life, sexual orientation, racial or ethnic origin, political opinions, religious or philosophical beliefs.

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 and biometric data. However, to the best of our knowledge, there aren't any specific data protection regulations set for 'Fem-Tech data' when collected and processed beyond health and medical clinics.

4.2 Swiss Federal Act on Data Protection

Switzerland is not an EU member, and nor is it a member of the larger European Economic Area (EEA). Swiss companies don't have to obey the GDPR. However, they have to obey the GDPR when they are operating in the EEA. The main data protection law of Switzerland is the Federal Act on Data Protection (FADP). FADP's definitions include a category of sensitive personal data. Sensitive personal data is defined in four groups: data on (1) religious, ideological, political or trade union-related views or activities, (2) health, the intimate sphere or the racial origin, (3) social security measures, and (4) administrative or criminal proceedings and sanctions. Accordingly, in addition to valid consent for personal data, consent must be given expressly in the case of processing sensitive personal data or personality profiles. Similar to the GDPR, the FADP gives sensitive data more protection.

Switzerland is implementing new legislation to better protect its citizens' data: the new Federal Act on Data Protection (nFADP), will come into effect on 1st Sep 2023. This revision was intended in particular to bring it closer to European

[12] Brave.com

[13] reports.exodus-privacy.eu.org/en/

[14] 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/

data protection legislation. One of the main changes is in the definition of sensitive data. These categories of personal data will continue to be considered sensitive under the Revised FADP. For instance, the Revised FADP will add two new categories: genetic data and biometric data that uniquely identify an individual.

Both GDPR and nFADP mandate a Data Protection Impact Assessment (DPIA) on special category and sensitive data. DPIA is a process to help companies identify and minimise the data protection risks of a project[15]. In general, by going through the guidelines and the description of data protection laws, we did not find any explicit mention of the FemTech keywords in the FADP. We also observed that the FADP is less expanded, developed, specified, and potentially enforced when it comes to sensitive data.

4.3 UK Medical Devices Regulations 2002

The Medicines and Healthcare Products Regulatory Agency (MHRA) is an executive agency of the Department of Health and Social Care in the UK which is responsible for ensuring the safety of medicines and medical devices. Their website provides a range of guidance[16] and regulations concerning health and medical services. MHRA has a guidance document on medical device stand-alone software including apps. It was published in 2014 and updated in 2022. It is clarified that "a medical purpose is determined by what the manufacturer states in the device's labelling, instructions for use and any promotional materials." It is a helpful document to guide developers identify how to progress within the regulatory environment and to distinguish whether the app falls within the scope of being a 'medical device'. If the device or app is a medical device then it must comply with the Medical Devices Regulations 2002[17]. This regulation is more than 20 years old and does not provide any content on the SP aspects of modern medical devices e.g., apps and connected devices. There is also no mention of FemTech-related data.

More recently, the MHRA is working on a new Software and AI as a Medical Device Change Programme[18] where one of its 11 work packages (WP5) is "Cyber Secure Medical Devices". This WP's deliverables include: (1) Secondary Legislation (Cybersecurity requirements for medical devices and IVDs (in vitro diagnostic medical devices)), (2) Regulatory Guidance (Guidance elucidating cybersecurity requirements for medical device and IVDs), (3) Best Practice Guidance (Management of unsupported software devices), (4) Processes (Reporting of relevant cybersecurity vulnerabilities).

4.4 Regulation (EU) 2017/745 for Medical Devices

The UK has been complying with EU medical and health regulations for years. However, due to Brexit, the UK does not necessarily comply with EU medical regulations anymore. For medical devices, Switzerland follows what is specified by the EU system of compliance assessment and certification, based on bilateral agreements. Hence, we also review the EU Regulation for Medical Devices. In the EU, medical devices must undergo a conformity assessment to demonstrate they meet legal requirements to ensure their safety and performance as intended. They are regulated at the EU Member State level, but the European Medicines Agency (EMA) is involved in the regulatory process. The Regulations on Medical Devices (Regulation (EU) 2017/745) and on In Vitro Diagnostic Devices (Regulation (EU) 2017/746) changed the European legal framework for medical devices, coming into effect in 2021 and 2022, respectively. In this section, we focus on the former.

This regulation defines 'medical device' as "any instrument, apparatus, appliance, software, implant, reagent, material or other article intended by the manufacturer to be used, alone or in combination, for human beings for one or more of the following specific medical purposes." They include diagnosis, prevention, prediction, monitoring, prognosis, treatment, alleviation, and compensation of disease, injury or disability, investigation, replacement or modification of the anatomy or of a physiological or pathological process or state, providing information by means of in vitro examination of specimens derived from the human body (e.g., organ, blood and tissue donations). They add that "devices for the control or support of conception" shall also be deemed to be medical devices. The following products shall also be deemed to be medical devices. It defines an 'invasive device' as "any device which, in whole or in part, penetrates inside the body, either through a body orifice or through the surface of the body". This regulation also applies to clinical investigations concerning such medical devices.

As general requirements for Electronic programmable systems, this document briefly says that for software devices or those that incorporate software, the development and risk management (i.e., information security, verification and validation) should be according to the state-of-the-art practices. The general safety requirements take into account the intended purpose which is set by the manufacturer. The parts related to risks and risk management are for safety risks and there is no mention of SP risks. Article 110 of this regulation is on data protection stating: "(1) Member States shall apply Directive 95/46/EC to the processing of personal data carried out in the Member States pursuant to this Regulation. (2) Regulation (EC) No 45/2001 shall apply to the processing of personal data carried out by the Commission pursuant to this Regulation." Note that the GDPR supersedes the Directive 95/46/EC

[15] ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

[16] gov.uk/government/publications/medical-devices-software-applications-apps

[17] legislation.gov.uk/uksi/2002/618/contents/made

[18] gov.uk/government/publications/software-and-ai-as-a-medical-device-change-programme/

Table 2: Data collected by FemTech IoT devices and apps. Devices with X are not connected to their associated apps. Android App categories include: Health and Fitness = HF, Medical = M, Entertainment = E, and Tools = T.

Device/App	(1) Elvie Pump	(2) Daysy Cycle	(3) Lady Comp Fertility	(4) Hidrate Bottle	(5) Perifit Kegel	(6) Frida Sex Toy	(7) Livia Pain Reliever	(8) Balance Menopause	(9) Daviky Pill Organiser	(10) Ivy Health Tracker
Device	✓	✓	✓	✓	✓	✓	X	no	X	✓
App	✓	✓	no	✓	✓	✓	✓	✓	✓	✓
Category	HF	M	-	HF	HF	E	E	HF	T	HF
Download #	100k+	50k+	NA	100k+	100k+	100k+	10k+	100k+	500+	1M+
User data										
User	✓	✓	✓	✓	✓	✓		✓	✓	✓
Contact	✓	✓		✓	✓	✓		✓	✓	✓
Lifestyle			✓	✓				✓		✓
Period		✓	✓		✓			✓		✓
Pregnancy				✓						✓
Nursing	✓			✓						
Reproductive		✓			✓			✓		
Sexual		✓	✓		✓	✓		✓		
Medical info					✓			✓	✓	
Physical					✓			✓		✓
Emotional					✓			✓		✓
Data about others										
Partner		✓			✓	✓				
Social media		✓		✓	✓	✓				
Child	✓									
IoT/Mobile device's resources										
Storage		✓		✓	✓	✓	✓	✓	✓	✓
Contacts		✓		✓	✓					✓
Accounts				✓						✓
Settings		✓			✓		✓			
Cam/mic		✓				✓	✓		✓	
WiFi	✓	✓		✓	✓	✓	✓	✓	✓	✓
Location	✓	✓		✓	✓	✓	✓		✓	✓
Bluetooth	✓	✓		✓	✓	✓				✓
NFC				✓						
Sensors	✓	✓	✓	✓	✓		✓			✓

and repeals Regulation (EC) No 45/2001.

Overall, we did not find any direct mention of FemTech-related data and its protection in these regulations. Similar to the UK MHRA, the European Commission also has a guidance document on Qualification and Classification of Software in Regulation[19] (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR, released in Oct 2019. In comparison, we found the UK guidance more comprehensive in terms of helping developers decide about the intended use of their product as a medical device.

5 Analysis of FemTech Systems

In this section, we present the results of data collection and tracking practices as well as the privacy policy review.

5.1 Data Collection

We examined what types of data these devices (Fig. 1) collect, as presented in Table 2. We broadly categorise this data into three groups: user data, data about others, and device/phone data. Our examinations show that **user data** include, but are not limited to: Name (e.g., 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

[19] ec.europa.eu/docsroom/documents/37581?locale=en

Table 3: Tracking practices of apps and websites

no.	Product	Exodus trackers & permissions	Brave Trackers
1	Elvie Smart Pump	2, 13	6
2	Daysy Cycle Computer	1, 35	1
3	Lady Comp Fertility Tracker	NA	1
4	HidrateSpark Smart Bottle	7, 25	70+
5	Perifit Kegel Trainer	8, 36	31
6	Frida (Vibio) Sex Toy	2, 39	3
7	Livia Menstrual Guide App (Associated with Pain Reliever)	7, 35	9
8	Balance Menopause App	2, 27	2
9	Daviky Pill Organiser	0, 6	2
10	Ivy (Bellabeat) Health Tracker	9, 23	10

results, due dates, IVF), Nursing (e.g., time, volume, pain) Reproductive organs (e.g., cervical mucus, biofeedback, 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), Emotional symptoms (e.g., happy, anxious). These systems also ask for or automatically collect **data about others** including: Baby/ 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 about the medical history of the user's family. Finally, these systems also have access to the **devices' resources** 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).

For example, Daysy Cycle Computer, Hidrate Spark3 Smart Bottle, and Perifit Kegel Exerciser collected data in all categories (user, partner, and device) quite intensively. There were also some devices which collected minimal data. For instance, Lady Comp Fertility Tracker collects some form of user data (e.g., age), cycle information, sex, and has a thermometer to measure user basal temperature. This device does not offer an app and has a memory for a year. The manual suggests that this data can be backed up by connecting the device to a PC via a cable. However, via testing, we could not use such a feature. Note that Table 2 only represents the data collected by the device and app itself and does not show the data that may be collected via the websites e.g., for purchasing, creating a profile account for networking, and subscribing. For instance, the Livia Menstrual Pain Reliever device does not collect any data about the user, though its associated app (which is not connected to the devices) does. Also, its website requires user and contact information for purchasing and subscription and offers a review platform via a third-party service too.

As can be seen, not only do these systems collect data about the user (and others), the majority of them have access to mobile and device resources too. Some of these permissions are marked as dangerous according to Google's protection levels. If not justified well, the risks of access to storage, contacts, camera, microphone, and location are more visible. However, specific permissions such as access to system Settings and other Accounts on the device also impose SP risks. Similarly, there is a body of research (e.g., [2]) on how sensors can be used to break user privacy. This can become more critical in FemTech systems since they are associated with user health.

5.2 Privacy Consent, Privacy Policy, and Tracking Practices

As demonstrated in Table 4, all the apps and websites that we studied appear to violate the GDPR in terms of asking for valid consent. They either nudge the user into accepting a highlighted accept, limit the access behind a privacy notice wall, bundle the privacy notice with other matters (e.g., terms and conditions), or don't provide any privacy consent. The only exception is the Balance Menopause App which presented valid consent. However, its website did not.

In addition, our review of the privacy policies of these apps indicates that 4 apps included a reference to or a description to FemTech-related data. For instance, the DaysyDay app highlights that “Within this framework of the contractual relationship between you and us, health data such as your body temperature, menstruation, etc. may also be processed. For such processing, we need your explicit consent. By submitting this data, you are granting us that consent." Yet, they also say: “Our online services are not subject to HIPA". These statements are problematic since explicit consent is in conflict with obtaining consent via submitting such data. Similarly, Prifit's privacy policy explains “Sensitive personal data" which is in accordance with the GDPR special data category and lists the data items that the app collects. However, it does not clarify how such data is given extra protection. Balance app's policy has a dedicated section for “health data" by defining it and explaining their approach regarding explicit consent for such data. However, again, it is not clear how such data is treated with care. Bellabeat's policy has a similar content on defining sensitive personal data to Prifit. It then says: “If the information we collect is health data or another special category of personal data subject to the European Union's General Data Protection Regulation, we ask for your explicit consent to process that kind of data. We acquire this consent separately when you take actions resulting in our receiving the data, for instance when you use the menstrual calendar feature". However, when trying to use the app by signing up via email, another Privacy Consent wall was shown which required the user to agree to tick two boxes: one general privacy policy and terms of use and one stating: “I agree to the processing of my personal health data for providing me Period Diary app functions, See more in Privacy Policy".

Table 4: Privacy notice of apps and websites and GDPR violations. The bold options in the Website cookie notice column is the highlighted option in the notice

no.	Product	FemTech data reference in Privacy Policy	Android App Privacy Notice [Place]	Violation	Website Cookie Notice & Options	Violation
1	Elvie Smart Pump	No	I agree to Elvie's terms of use & privacy policy [Sign-up page (wall)]	✓	**Accept All**, Customise	✓
2	Daysy Cycle Comp	Yes (health, body temp, menstruation)	I've seen the imprint & accept privacy policy [Welcome page (wall)]	✓	**Accept**	✓
3	Lady Copm Fertility Tracker	NA	No App	NA	**Accept**	✓
4	HidrateSpark Smart Bottle	No	I agree to terms of service & privacy policy [Sign-up page (wall)]	✓	Preferences, **Accept**	✓
5	Perifit Kegel Trainer	Yes (health, sex, menopause, health, gender, height, weight)	..., you expressly agree to collection of your health data, ... [Sign-up page (wall)]	✓	**Allow all cookies**, Cookie settings	✓
6	Frida (Vibio) Sex Toy	No	I have read & understood the Terms & Conditions and Privacy agreement [Sign-up page (wall)]	✓	No Notice	✓
7	Livia Menstrual Pain Reliever	NA	No privacy content	✓	No Notice	✓
8	Balance Menopause Support App	Yes (health, symptoms, medication, menopause)	(i) View our privacy policy [(Welcome page)] (ii) I accept that you may use the data I share for the above purposes [(Second page)]	No	Save and close, **Accept all cookies**	✓
9	Daviky Pill Organiser	No	No privacy content	✓	No Notice	✓
10	Ivy (Bellabeat) Health Tracker	Yes (health, exercise, steps, heart rate, pregnancy, weight, sleep)	By continuing you agree to Bellabeat's Terms & Conditions & Privacy Policy [Sign-up page (wall)]	✓	No Notice	✓

Table 3 shows the apps and websites of all these products and the trackers. Our Exodus analysis revealed that these apps have between 1 to 9 trackers. In addition, the majority of these websites are tracking the users before the user engages with the cookie notice. One particular website (hidratespark.com/) increased the number of these trackers to more than 70 (and counting) while we kept the website open and without any interaction with it. It also attempted to use motion sensors on a mobile device if accessed from one. In contrast, the Daysy Cycle Computer and Lady Comp Tracker both included only one tracker (Google Tag Manager).

6 Discussion

While there are some efforts to enforce the law in the FemTech space (e.g., the ICO's recent project on auditing FemTech apps[20]), here we discuss that a more proactive approach to policy-making and enforcement is needed in this sector.

6.1 Gaps in the Related Regulations

Our critical review of FemTech-related regulations shows that they are inadequate in addressing the risks associated with these technologies. The EU and UK medical devices regulations don't have any references to FemTech data and user protection. The GDPR and Swiss FADP have references to sensitive and special category data which overlap with FemTech data. Yet, there are several areas for expansion and improvement.

While GDPR gives extra protection to special category data, there are 10 exceptions: 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 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. The exceptions of data protection regula-

[20] datamatters.sidley.com/2023/04/20/femtech-has-been-warned-uks-ico-indicates-closer-scrutinization-of-femtech-apps/

tions (e.g., GDPR) are indeed debatable. While the analysis of these exceptions in the wild is beyond the scope of this paper, we believe that this is an area that will unfold significantly in the future. For instance, consider the first exception: explicit consent. Given the sensitive nature of FemTech data and its differential and complex risks and harms [8], how do we guarantee that the user is fully aware of the consequences of such consent and make an informed decision? More research is needed for filling in these research gaps.

6.2 General Data Regulations vs. Medical Devices Regulations

When reviewing the current general data protection regulations and the medical ones, we find several gaps and disconnections between the two sets of regulations. We would expect a higher level of safeguarding in these products where personal health data is recorded, even if the app does not fall within current medical device definitions and regulations. This is supposed to be covered by the special categories of data in the general data protection laws. However, in practice and based on our experiments, it is not enforced properly. For instance, we did not find any appropriate consent in apps and websites tested and whether or not any extra protection is given to sensitive FemTech data. As we discuss in [1], the fact that these products collect data about others (partner, baby/child, family, etc.) adds to these complexities.

When registering an app in the app store, the developers select the most appropriate app category. However, due to the ambiguity in the definition of these categories, the doors are open to potential misuse and gaming by the registrant. At the time of this writing, there are 38 categories on the Google Play App Store including 'Medical', and 'Health and Fitness' categories. Yet, as reported in Table 2, only one of these apps (#2) is listed as medical, 5 listed as health and fitness, and the rest include 'Entertainment' or 'Tool'. Miscategorising an app which contains medical records (such as user's medical conditions and medicines, or family history) as Health & Fitness or other groups would enable the developers to avoid the potential consequences, for example, of remaining in the app market without drawing significant attention to it. As long as such apps and services make only general wellness claims -like tools, entertainment, health and fitness, they do not need to be vetted by health regulators or as seriously as one expects by the mobile app store.

The UK MHRA is developing a new Software and AI as a Medical Device Change Programme, where apart from a dedicated work package to cybersecurity (WP5), it also has one on Classification (WP2). The problem statement says: "Currently, the Medical Device Regulations 2002 (as amended) do not classify software proportionate to the risk it might pose to patients and public safety." We believe that such efforts are required immediately to protect citizens against these risks.

6.3 Non-compliant Practices

We identified a range of inappropriate SP practices in a subset of FemTech systems. We showed that they do not present valid consent, the do not give extra protection to sensitive data, and track users without consent. These are some of the non-compliant practices within the current regulations. In [10], we discuss that not only is such intimate data collected by FemTech systems, but also this data is processed and sold to third parties[21]. In [8, 9], we have discussed at length that complex harms and risks such as the re-identification of individuals based on health data [4] can differentially impact the users.

In addition, most of these products do not need a wide range of information about the users to deliver their services. Yet they continue to collect such sensitive data. Some of these practices could be due to factors such as copying and pasting an app code by developers without considering privacy-by-design principles. For instance, the app associated with Livia period pain reliever (which is approved by the FDA), is simply a guide on the use of the device. While interacting with it, we did not notice any data collection or permission requests. Yet, when we checked the app's permissions, we noticed that the camera, music and audio, notifications, and photos and videos are listed. If turned on, this app is able to collect such data. This is clearly a bad practice from the developer side.

Non-compliance or poor adherence to laws and standards may arise for many reasons. There may be unintentional oversight or a deliberate attempt for commercial or other purposes. The developers themselves may be unaware of best practices and regulations in the area. Different solutions (websites, apps, IoT devices) developed in different territories may be subject to different regulations, yet regulators may not have the powers or resources to certify compliance or investigate potential non-compliance where no certification process exists. This might be the time to focus on more sectorial and domain-specific data protection regulations as we discuss next.

6.4 Domain-specific Regulations

As discussed in this paper, two sets of regulations apply to FemTech solutions: general data protection regulations and medical and health regulations. However, as shown, alone or combined they fail to protect the user from malicious practices. In addition, a key complement to regulations is systems of certification, compliance testing and policing/penalties. Accordingly, providers and developers need to be aware of the regulations, guidance and best practice and have appropriate tools to develop and evaluate products. Currently, there are no entities well-equipped to provide such services.

We acknowledge that the legal framework of the medical and health sector is a combination of laws, standards, certifica-

[21] ftm.eu/articles/your-intimate-data-is-being-sold

tions, and beyond. For instance, ISO 13485 is specifically for products that fall within the criteria for a ‘medical device’. Implementation of ISO 13485 tends to draw with its alignment to data standards, as such products are subject to clinical trial validation, governed by ethics committees, who would likely question marginal data practices and so has a wider influence on the company and its marketing behaviour. Companies often deliberately frame their products as ‘non-medical’ and e.g., as ‘wellbeing’ to avoid being subject to the medical device regulation. Hence, the period and cycle tracking apps are on the market free from regulation as it can be argued that the information is not used for clinical decision-making and guidance for treatment. Whereas ovulation tests (aka class I in medical devices regulations)/pregnancy tests (class II) are used and subject to regulation, even if ovulation tests are then associated with an app just for the purpose of cycle tracking.

We are now seeing more efforts in the policymaking space to recognise these issues. For instance, the EU is aiming to foster common European data spaces. Data spaces are data ecosystems, often domain-specific, in which data sharing should be possible between actors. One of the data spaces is the European Health Data Space[22]. This proposal is still under review and it is unclear when and how it will be implemented and enforced, let alone what kind of organisations fall under these definitions. We believe that the medical and health space is in need of domain-specific and sectorial regulations with attention to the needs of marginalised user groups such as women and those with physical and mental ability limitations.

7 Conclusion

The SP issues around FemTech can lead to differential harm where complex risks are enabled by many factors including gaps in the regulations, non-compliant practices, the lack of enforcement, and limited research and guidelines for secure, privacy-preserving, and safe products. We reviewed the regulations related to FemTech in the UK, EU, and Switzerland and identified the gaps. We ran experiments on a range of FemTech devices, apps, and websites and identified several exploitative practices. We discussed our results and suggested that policymakers explicitly acknowledge and accommodate the risks of these technologies in the relevant regulations.

Acknowledgement

This work was supported by the ETH Future Computing Laboratory and was partially conducted when the first and second authors were working at ETH Zurich in 2022. This work has been supported by the PETRAS National Centre of Excellence for IoT Systems Cybersecurity, funded by the UK EPSRC under grant number EP/S035362/1.

References

[1] T. Almeida, L. Shipp, M. Mehrnezhad, and E. Toreini. Bodies like yours: Enquiring data privacy in femtech. In *ACM NordiCHI*, 2022.

[2] P. Delgado-Santos, G. Stragapede, R. Tolosana, R. Guest, F. Deravi, and R. Vera-Rodriguez. A survey of privacy vulnerabilities of mobile device sensors. *ACM Computing Surveys (CSUR)*, 54(11s), 2022.

[3] 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.

[4] B. Goldacre, J. Morley, and N. Hamilton. Better, broader, safer: using health data for research and analysis. *A Review Commissioned by the Secretary of State for Health and Social Care*, 2022.

[5] N. Mcdonald and N. Andalibi. “i did watch ‘the handmaid’s tale’”: Threat modeling privacy post-roe in the united states. *ACM Transactions on Computer-Human Interaction*, 2023.

[6] C. McMillan. Rethinking the regulation of digital contraception under the medical devices regime. *Medical Law International*, 2023.

[7] M. Mehrnezhad. A cross-platform evaluation of privacy notices and tracking practices. In *IEEE EuroS&P Workshop, EuroUSEC*, 2020.

[8] M. Mehrnezhad and T. Almeida. Caring for intimate data in fertility technologies. In *ACM CHI*, 2021.

[9] M. Mehrnezhad and T. Almeida. "my sex-related data is more sensitive than my financial data and i want the same level of security and privacy": User risk perceptions and protective actions in female-oriented technologies. *arXiv preprint arXiv:2306.05956*, 2023.

[10] M. Mehrnezhad, L. Shipp, T. Almeida, and E. Toreini. Vision: Too little too late? do the risks of femtech already outweigh the benefits? In *EuroUSEC 2022*, 2022.

[11] C. Rosas. The future is femtech: Privacy and data security issues surrounding femtech applications. *Hastings Business Law Journal*, 15(2), 2019.

[12] 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), 2022.

[13] 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.

[22] health.ec.europa.eu/ehealth-digital-health-and-careeuropean-health-data-space_en