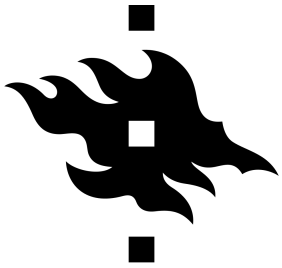

HELSINGIN YLIOPISTO
HELSINGFORS UNIVERSITET
UNIVERSITY OF HELSINKI

“Your period starts in two days”
Risks of period-tracking post Roe v. Wade

Sini-Marja Ant-Wuorinen, Maria Knaapi, Heli Koskela, Emma Lindberg, Anni Lintula & Linda Palenius

Faculty of Social Sciences, University of Helsinki
Master’s Programme in Global Politics and Communication

Abstract

The future of period-tracking applications, or *Femtech*, is currently under fire after the overturning of Roe v. Wade by the Supreme Court of the United States in June 2022. In this changing landscape of reproductive rights, questions are being raised about the need for more regulation and ethical standards. Period-tracking apps, which usually help users make decisions about their reproductive health, are now a potential threat to women's bodily autonomy and the right to privacy, as well as a means of control, surveillance, and even prosecution by authorities. In this paper, we aim to map out the various risks relating to this progress post Roe v. Wade and raise questions about the future. Is sharing health data with period-tracking apps at all safe with the unknowns of machine learning? What could be done to protect users, and what precautions can users themselves take to protect their data and themselves?

Keywords: Femtech, period-tracking apps, surveillance, privacy rights, machine learning

1. Introduction

As the use of artificial intelligence and machine learning keeps getting more common, different technologies are becoming exceedingly enhanced. As for female health, period-tracking applications have been developed to help keep track of the menstrual cycle and different aspects related to it. However, the privacy of the intimate data users share with the apps has been called into question – even more urgently with the overturning of Roe v. Wade in the United States. This paper seeks to approach this topic from different angles, and to answer the question: could the data period-tracking applications collect be used to target and punish women seeking an abortion in the US?

In chapter 2 of this paper, we overview three current developments and public debates in the US. These include restricted "Post Roe" abortion rights, the commodification of abortion seekers' data, and the concerns raised by data demands and surveillance by the government. In chapter 3, we address the question of how it is possible to make evaluations of data sharing safety in the new technological and legal environment. The section focuses especially on machine learning and the possibility of detecting or predicting abortion. Section 4 approaches the topic in respect of control. First, it suggests that period-tracking apps are used because they create a sensation of being in control of one's own body. Second, we proceed to demonstrate that gaining this control is debatable – instead, the use of period-tracking apps may lead to losing control when personal data is shared with third parties.

Section 5 takes a look at Femtech as an industry with its promises and issues. Femtech has noble goals of narrowing the health data gender gap caused by medical research that disregards women's health. However, the promises of feminist empowerment crumble under the lack of regulation to keep user data safe. Section 6 analyzes the data privacy and safety of period-tracking apps. We discuss whether women should switch out their current apps in search of better data privacy – or to delete them altogether. In section 7, we present future threats and opportunities of period-tracking apps and Femtech in general from the perspective of regulation and legislation. The need for a more critical approach and further technological development – related not only to data processing, but to education too – is also brought out.

2. Background: Abortion rights and data-related investigation methods of the law enforcement

Heli Koskela

Law and data privacy experts have feared that with the United States Supreme Court's decision to overturn Roe v. Wade, people in the US might end up in a dystopia. A dystopia, where not only would they return to the time before 1973, when abortion was not a national fundamental right, but move to an even darker future, where those facing termination of pregnancy would face digital surveillance, and could be accused of a crime, even the murder of a fetus, based on their digital footprint. (See Fowler, 2022; Fox Cahn, 2022.)

Where do these dystopian thoughts derive from? The goal of this section is to provide context and argue for the need of risk assessment of period-tracking applications, by creating an overview of three societal developments and public debates in the United States.

2.1. Restricted abortion rights "post Roe"

With its decision Dobbs v. Jackson Women's Health Organization on June 24, 2022, the Supreme Court of the United States overturned the decisions Roe v. Wade (1973) and Planned Parenthood of Southeastern Pennsylvania v. Casey (1992), which had guaranteed constitutional abortion rights before the viability of the fetus. The power to regulate abortion was returned to the people and their elected representatives. (Dobbs v. Jackson Women's Health Organization, 2022.)

The decision sparked a huge public debate and movement, and divided the United States, including Presidents Biden and Trump, into two camps between mainly conservative and religious groups that emphasize the rights for life of the fetus and liberal groups that advocate women's self-determination rights related to their own bodies.

Following the decision, several states banned or greatly tightened abortion rights, and many abortion clinics closed their doors. There were also reports of confusion when the implementation of new banning laws was soon suspended due to opposition. (See Atkins, 2022; Sneed 2022.) Currently, abortion is prohibited in fourteen states completely or from the 6th week of pregnancy onwards (Väntönen, 2022).

The 1973 Roe v. Wade decision was widely considered as the backbone of reproductive abortion rights, even though the implementation of the rights had varied even with the federal law in place. (See Fowler, 2022).

Almost half of the abortion service providers had closed the doors since the early

1980´s until 2017 (Diamant, 2022). This has led not only to the so-called abortion tourism to states considering abortion legal, but also to the growing importance of the internet in planning and carrying out abortions. The trend is estimated to accelerate with the US Supreme Court´s decision of June 24th.

As women aged 20-29 years form the largest group of those having abortion, (Diamant, 2022) and 94% of women in this age group have a smartphone (Bankmycell, 2022), it is no wonder that organizations promoting the safety and privacy of abortions advice on how to try to secure one´s smartphone and its contents, from outside parties like US authorities or other pressure groups (See Digital Defense Fund, 2022). US women also use period-tracking apps mostly with the smartphone.

2.2. Abortion seekers' data as a possible commodity

As the United States has heavily digitized in recent decades, but lacks federal data privacy law, a critical understanding of user-generated data and its possible collection, storage and sharing to third parties has entered the public debate.

Non-governmental organizations have warned about data privacy protection deficiencies related to period-tracking apps after they began to become popular in 2012-2013 (Amelang, 2022).

Whether it is the abortion seeker's sensitive information on period-tracking applications, phone calls, e-mails, text messages, photos, internet searches, purchases paid with a credit card or user´s physical location information - the data may form an archive of several years, possibly stored on the service provider's server or in the cloud, which then may be commodified when shared to third parties.

Collecting and using private data against abort seekers or providers is not a new phenomenon. Opponents of abortion have used data to reveal their names, harass, and even pressure them. (Fox Cahn, 2022.)

There is also a critical debate on information or data brokers business in the US. For example the American company Acxiom has said that it has collected data from 2.5 billion people, 11,000 data points per person (Singer, 2012.). Databrokers sell or license information for various purposes to third parties, including the US administration and law enforcement (Sherman, 2021).

2.3. Data-related criminal investigation methods

The data-related criminal investigation methods used by US law enforcement are also causing great concern. The "dystopians" refer to the criminal investigations related to alleged illegal abortions or fetal homicides during the 2010's (See Fox Cahn, 2022). Some investigations by US law enforcement used user-generated data as evidence and led to convictions.

In 2012, Pennsylvania officials prosecuted a mother for purchasing an abortifacient online and administering it to her teenage daughter, securing a sentence of 9 to 18 months in prison. Indiana prosecutors used Purvi Patel's text messages in 2015 to convict her of murder for terminating her pregnancy with abortifacients ordered from Hong Kong.

Mississippi police used a woman's own search history to charge her with second degree murder following a miscarriage in 2018, relying on queries about miscarriages and how to purchase abortion-inducing pills. And in 2019, the Food and Drug Administration successfully charged a New York City woman with illegal online sales of abortifacients, following PayPal's termination of her account (Fox Cahn, 2022).

The law enforcement´s right to receive information from service providers, including companies offering period-tracking apps, is regulated by the law America's Stored Communications Act, passed in 1986. (Walker, 2021.)

Most of the data is indeed available to the law enforcement, the information depending on the data request submitted by the authority to the service provider, be it a subpoena, court order or warrant. For sensitive data investigators need a warrant issued by a judge. Evidence suggesting that the subject committed a crime is needed. (Nicas, 2021.)

What may be alarming in terms of transparency, the law enforcement has increasingly used so-called non-disclosure orders to acquire user data “in secret” without the subject of the investigation finding out about the data request. These orders can be submitted without a judge's decision (See Walker, 2021). For obtaining the data from data brokers, the authority often does not need a court-issued permission, as the data is considered to have been collected from public sources.

Recently, it was revealed that eighteen local, state or federal police or authorities have acquired a mass surveillance technology service produced by a data broker. The service allows one to monitor the geolocation without the knowledge of the users (See Guariglia, 2022). And not only the individual under investigation, but of all IP addresses that have been in the past years, or in real time, near a specific abortion clinic, for instance.

The combination of this kind of less transparent and more mass-oriented data with for

example, data produced by period-tracking applications in those states prohibiting the abortion, worries many. US Senator Warren introduced on 15th of June 2022 the *Health and Location Data Protection Act*, legislation that would ban data brokers from selling this, some of the most sensitive data available about everyday Americans (Warren et al, 2022).

3. Theoretical background: Machine learning and period-tracking apps

Emma Lindberg

The relationship between the legal system and available technologies has become a growingly interesting one. Speaking strictly in terms of the law, the decisions to restrict abortion rights following the overturn of Roe v. Wade is hardly one of a kind in a historical perspective (Hull & Hoffer, 2010, p. 11). However, considering the current technological environment and the available means of surveillance, we argue the situation today is not comparable with the early twentieth century United States, where abortion had reached nationwide criminalization with only minor exceptions (Joffe et al. 2004). Instead, we argue, the overturn of Roe v. Wade should be considered as a unique case.

The improvements in machine learning, a sub-discipline of artificial intelligence, are offering new efficient means to detect and predict violations of the law and could introduce significant changes to law enforcement. Together with the availability of large amounts of data, machine learning capabilities offer new means for surveillance. However, it might also introduce privacy concerns and undermine the balance between ensuring national security on the one hand and individual privacy on the other hand (Verhelst et al. 2020). Improved means of surveillance could also imply that laws are becoming more binding and that changes in the legal environment should therefore be considered with greater care.

As digital data is found at the center of machine learning applications, protecting personal data has become a serious concern (Verhelst et al. 2020). As will be discussed further in chapter five, new applications for reproductive health data are being developed parallel with the rise of Femtech. In the light of changing legal environment and technological development, a relevant question is raised of how much and what kind of data is sufficient to make the conclusion that a person has had or is about to have an abortion (Popli & Bergengruen, 2022). We could make differing assessments on what information we believe to be sufficient to make this conclusion, and potentially even find some pieces of information we would all regard as necessary for this deduction. However, machine learning could disregard all these human evaluations and follow its own logic of inference through

identifying new relationships between grains of information, details which humans would disregard as insufficient or irrelevant for the inference (Hildebrandt, 2016). To approach the question if sharing personal data, such as menstrual data, is ever safe, we will focus next on the ability of machine learning to process large datasets, find connections in data and make conclusions and predictions.

3.1. What is machine learning: what do we know, what won't we know?

The term "machine learning" does not follow the human idea of learning but instead is used to describe a complicated computing process (Boulanin, 2019). In this process, a machine learning algorithm processes large amounts of data to regroup information, make comparisons and to find statistical connections between data points (Boulanin, 2019). Based on these capabilities, machine learning can also make predictions of future actions by using statistics (Boulanin, 2019). One of the key features of machine learning is that it is operating on feedback loops, which enables it to improve its performance (Hildebrandt, 2016).

The dependency of machine learning on large data sets explain why it has become the most prominent approach in AI engineering during the last decade simultaneously with the rapid growth in the amount of available digital data. Even though enormous amounts of data are available for machine learning processes, this requirement of large amounts of quality data has also been considered the technology's limitation. If the data is no longer of quality and the masses of data are not at a sufficient level the machine learning doesn't function as wished. (Boulanin, 2019.)

Another considered limitation on machine learning is the unpredictability of its inference process. This is a consequence of the fact that the logic behind machine learning algorithms is complicated for humans to understand. This complicated learning process has been described as a black box: the only stages of the process at our disposal for further exploration are the input and the output. This might question the reliability of the conclusion as the inductive process cannot be examined in detail and therefore the possible biases and defects cannot be thoroughly examined, and the credibility of the outcome evaluated. (Boulanin, 2019.)

3.2. Evaluating safety for data sharing

The ability of machine learning to identify unforeseen relations between data points can be utilized by machine learning to make predictions on behavior (Boulanin, 2019). This ability

to discover correlations could have various valuable applications and could be used for instance to diagnose illnesses (Hildebrandt, 2016). In the light of the new legislation on reproductive rights, finding unforeseen relations from menstrual data could potentially be exploited to make interpretations on reproductive health, most interestingly identifying pregnancy or abortion. In addition, machine learning has demonstrated its advance in reasoning by successfully deriving identities from originally anonymous data, which highlights why providing sensitive data, even anonymous, is a cause for concern (Verhelst et al. 2020).

The predicting ability of machine learning has already been successfully applied for example in a model on predicting car thefts by recognizing high risk locations and a typical time for a crime to occur (Verhelst et al. 2020). Similarly, machine learning algorithms can be trained to identify people as potential threats for safety, based on their personal data (Verhelst et al. 2020). Both of these approaches could be applied to detecting or predicting abortions especially if in addition to digital footprint from various digital activities, there is personal data on periods available.

If we consider data sharing concerns in general, we could note that identifying abortion does not necessarily require machine learning capabilities. Making assumptions about abortion could be done with a more simplistic automation algorithm when given sufficient data. This algorithm is called 'IFTTT' ("if this then that") due to its functioning logic (Halpern, 2014). Hand-coded IFTTT follows clear instructions formulated by humans with logic that is familiar to human deduction **(**Hildebrandt, 2016). This type of algorithm could for example process datasets and follow a rule: "See if a person is pregnant. If pregnant, see if the person gives birth approximately in nine months' time. If doesn't give birth in that time frame, notify authority". However, what makes machine learning distinct from IFTTT-algorithms is that it functions without comprehensive instructions for all the stages of action **(**Hildebrandt, 2016). This feature of machine learning opens doors for more complex tasks and countless applications (Boulanin, 2019).

Many of the fundamental elements of machine learning seem to make the task of evaluating whether data sharing is safe difficult if not impossible. The black box functioning logic of machine learning together with its ability to find unforeseen correlations would imply that even an expert on reproductive health would be unable to make a definite evaluation on what kind of personal data would be sufficient for machine learning to make conclusions about a person's abortions. This makes sharing period data concerning. The question seems not to be whether a conclusion about abortions based on a simple input data

can be made, but instead if we trust the instances holding this confidential information about us.

4. Who is in control?

Linda Palenius

Period-tracking apps, like other health related applications, provide information and data about one's body and its specific functions – in the case of period-tracking apps, they promise to identify and predict the length of a woman's cycle and the important dates related to it, such as ovulation. Thus, period-tracking is often about either preventing pregnancy or trying to conceive. However, using the apps that track periods have deeper implications than this.

4.1. Gaining control (of your own body)

First of all, the period-tracking apps enable the menstrual cycle to be measured in such a way that it can be transformed into quantitative data. This numerical data is seen as more objective and reliable than a woman's own sensations of her body, and therefore a better source of information when it comes to for example period and ovulation. As the special features of women's bodies, such as the menstrual cycle, are still seen as being uncontrollable, quantitative data that period apps provide give the impression of generating more scientifically based knowledge of one's body and thus it also creates a sense of control. (Lupton, 2015) On the other hand, besides making gathering specific information possible, period-tracking and other health related apps also reinforce the idea that the collection of very private data and the self-optimization by using this data to acquire control over the bodily functions is worth pursuing. (Ruckenstein, 2014) For examples of how the period-tracking app Clue encourages its users to self-optimize, see section 5.2. of this paper.

As a consequence, awareness of one's own bodily functions and menstrual cycle is a way to control oneself and the body. In this way, period-tracking apps create the sensation of gaining control of your own body – that *you* are the one in control. What is especially noteworthy of this kind of self-surveillance is that people contributing to it do not necessarily see themselves as worthy objects of surveillance (Best, 2010). It is not always clear that the data that creates the impression of having power over one's own body may in reality lead to being controlled by outsiders.

Moreover, it is questionable whether the apps actually work as efficiently as they

promise and whether the app users get the benefits they are looking for. The algorithms that the apps use vary between different app developers, they are not scientifically approved, and they often lack any quality control. The system behind the period-tracking is thus hard for the app users to understand, and their reliability in general has been shown to be debatable at best. For example, relying on a period-tracking app as a method of pregnancy prevention can lead to unplanned pregnancies. Furthermore, studies indicate that calendar-based apps often fail to predict the date of ovulation correctly, and lead to decreased chances of conceiving as the most fertile window of the menstrual cycle is misinterpreted. (Duane et al., 2016; Freis et al., 2018) It may be concluded, then, that the sense of control of one's own body and menstrual cycle that period-tracking apps create is not in fact based on reliable information, but that the feeling of control is rather illusionary.

4.2. Losing control (of your own body)

The question then arises: who is in control of the women using the apps? Unfortunately, but perhaps not very surprisingly, the remarkably personal data that the apps contain has not remained private in numerous instances. A study conducted by Privacy International[1] in 2019 revealed that multiple period-tracking apps had severe issues concerning user privacy. For example, some of them send information that could be characterized as very intimate directly to Facebook, without the app user even having to have a personal Facebook account. The study suggested that it was not only possible but very probable that private data of the millions of app users have been shared with Facebook and other third parties. (Privacy International, 2019.)

The information collected by period-tracking apps that is then shared with third parties can be used in various ways: marketing, pursuing political influence and even in legal matters, such as criminal charges, as is the case with the recent overturning of Roe v. Wade by the US Supreme Court. Targeted advertising is not further discussed here, but it is noteworthy that according to Princeton University assistant professor of sociology Janet Vertesi, in 2014 the marketing data of a regular person rose from 10 cents to 1.5 dollars if they got pregnant (Petronzio, 2014). This highlights the monetary value of the woman-specific data collected by period-tracking apps. With regard to criminal prosecution, it is questionable whether period-tracking apps are capable of withholding the privacy of their

[1] According to their website, "Privacy International (PI) is a registered charity based in London that works at the intersection of modern technologies and rights."

users. The overturn of Roe v. Wade means that as abortion becomes illegal in some states, companies may be legally required to share some of its users' data with the authorities. The period-tracking app Stardust has stated that the data it might be ordered to release will be encrypted and anonymous, thus securing the anonymity of its users (Cole, 2022). However, as also already mentioned in section 3 this paper, metadata that includes for example the whereabouts of an individual may be connected with the data of the period-tracking app, thus questioning the promise of anonymity (Privacy International, 2022) The consequences of overturning Roe v. Wade and the relation to period-tracking apps will be further discussed in section 6.

To conclude, what is especially remarkable about the current state of private health information, which includes data about menstrual cycle, is that it is no longer the individuals themselves who remain in charge of all the knowledge. In fact, it can be argued that the amount of information gathered by different digital devices and technologies that are now a natural and inseparable part of our everyday lifestyle is so great that digital databases know more about an individual than they themselves do. This, in turn, has a great impact on the overall formation of individual identities. (Bossewitch & Sinnreich, 2013)

Moreover, apps are not only useful assistants or easy entertainments, but, as Lupton (2015, 441) has expressed, "(…) they are also sociocultural products located within pre-established circuits of discourse and meaning." What this means is that apps are not value-neutral, nor can they be regarded as representing objectivity. They are created and used within already existing social constructions that include different discourses and value-systems. They may, for example, deepen already existing ideas of womanhood and women's sexual health, which includes the questions related to menstrual cycle, pregnancy and abortion. (Lupton, 2012, 2015) The question of control, then, is multifaceted, and has no clear answer. The issues of privacy and the overall reliability of the functionality of period-tracking apps raise great concerns. However, the aspect of female empowerment should not be overlooked, either. Next section will take a deeper look into this with regards to Femtech.

5. Femtech as an industry

Maria Knaapi

Femtech, as originally coined by Clue co-founder and former CEO Ida Tin, consists of "software, diagnostics, products and services, that use technology to support women's health"

(Folkendt 2019). It's an industry that has revealed an enormous demand for modern female health solutions: Femtech's current market size ranges from $500 million to $1 billion (McKinsey & Company 2022) and it's estimated to be worth up to $20 billion by 2032 (Future Market Insights 2022).

The world of medical research is still to this day dominated by studies only conducted on male subjects – being a woman, having estrogen, menstruating, and going through menopause are seen as distracting variables to be eliminated. Caroline Criado Perez points this out in her book *Invisible Women: Data Bias in a World Designed for Men* (2019, 157): the whole medical field views male bodies as the default that represents all of humanity, resulting in a huge data gap. This gap keeps influencing future research, making it inaccurate. Here Femtech has an opportunity to step up and bring female health data the attention it needs to ensure accurate and effective healthcare for the *whole* human population.

Femtech's potential doesn't come without complications. The industry markets itself as a tool for feminist empowerment by enhancing female autonomy through datafied self-knowledge – but is this really what's achieved? Overturning of Roe v. Wade raises even more concerns. Will Femtech still be able to hang on to its claims of empowerment when there's an increasing risk of sensitive data being handed over to the authorities? Will Femtech companies be able to keep theirs users safe from reproductive and data surveillance?

5.1. Feminist empowerment or data surveillance?

A discourse of *empowerment* dominates the marketing materials of most period-tracking apps. According to Hendl and Jansky (2022, 33), period-tracking apps make three major claims on how they empower their users: they allow users to *understand* their bodies better, to be in *control* of their bodies, and to take *ownership* of their reproductive health. This empowerment is a result of self-knowledge generated by the apps – of acquiring data-driven information about one's body – which strengthens individual autonomy and choice in reproductive health and life in general (Hendl & Jansky 2022, 39). The rhetoric of feminist empowerment has however been contested, as it's been suggested that the industry instead reproduces existing social inequalities by not recognizing socioeconomic and political factors that determine one's access to reproductive health, and by not taking into account the male-dominant nature of the tech industry (Hendl & Jansky 2022, 30).

Femtech can also be seen as contributing to the neo-liberal privatization of healthcare by shifting medical responsibility and healthcare labor onto the individual (Neff & Nafus

2016, 56). Gilman (2021, 113) suggests that the only way for Femtech to be truly empowering is to remove it from corporate interests: the apps may seem to be "free", but in reality they come with the hidden costs of privacy, autonomy, and justice. The fact that the apps function on the basis of data extraction also creates a structural power imbalance between those who collect data and those who data is collected from (Gilman 2021, 111). The quantified approach to female empowerment proves to be problematic as the apps often give inaccurate predictions, data is impossible to erase, and there's no real option to stop the tracking (Mishra & Suresh 2021, 600). These findings further point out the contradiction between Femtech's discourse of empowerment and its real material interests in data, surveillance, and profit. This tends to go unnoticed because the users don't view themselves as worthy of surveillance, although they are indeed participating in *self-surveillance* by logging their data into apps – as elaborated in chapter 4.1.

Femtech offers hope for a more equal and accessible medical future but it also brings about many new risks. The data gathered by period-tracking apps is by nature different from data produced by healthcare providers – Femtech apps are run by corporations trying to make a profit, not by medical professionals seeking to improve people's health. Money also rules in the medical world but what's crucial is that the apps lack sufficient and meaningful regulation and ethical standards, unlike the medical field. This leads to a situation where there's no real data privacy and therefore medical privacy, and where data meant to empower users becomes a possible tool for surveillance and control.

5.2. A look into the applications – Flo and Clue

Two of the most popular apps that focus solely on period-tracking are *Flo* and *Clue* which have 40 million and 11 million monthly active users, respectively, according to their websites (Clue 2022a, Flo 2022b). There are countless smaller period tracker apps, and period-tracking is also often a feature in more general health or wellness apps, such as Apple Health, to which both Flo and Clue allow you to sync your data to. Period-tracking apps act as a calendar where you can input your period flow days, and as a way to track other relevant symptoms such as pain, mood, sleep, sexual activity and contraceptives, among others. They analyze all data input and give the user insights on their reproductive and general health, as well as notifications – thus "Your period starts in two days". The apps also have options to utilize your data by sharing it in different ways: Flo allows you to download a report of your data that you can easily bring to a doctor in case of health concerns (Flo 2022a), whereas

Clue has a “Connect” feature which you can use to share your cycle with your friends, family, or partners (Clue 2022d). The latter is what Thomas and Lupton (2015, 6, 14) would call “thrills”: aspects of reproductive health and self-tracking that the apps represent in playful terms, as enjoyment, entertainment, and consumption, as opposed to the usual “threats” that can harm the reproductive body. These kinds of features have a two-fold effect where they make period-tracking more fun, but also further alienate users from the possible risks.

In addition to the traditional period-tracking mode which is free, both apps offer a paid-for option with extra features. *Flo Premium* gains you “A Daily Well-Being Plan”, “Video courses and expert content” and “Unlimited access to Flo Health Assistant” (Flo 2022c) for the price of 14.99€ a month or 32.99€ a year. *Clue Plus* gives users access to five additional modes for the price of 9.99€ a month or 39.99€ a year: Clue Period Tracking Plus, Clue Birth Control, Clue Conceive, Clue Pregnancy and Clue Postpartum (Clue 2022b). What is interesting in regards to the topic of this paper is the Clue Birth Control mode, which Clue promotes to be a digital contraceptive and a medical device approved by the United States Food and Drug Administration (FDA), soon to be launching in the U.S. (Clue 2022c). The possibilities of classifying period-tracking apps as *medical devices* are explored further in chapter 7.

Both Flo and Clue have added data safety statements to the front pages of their websites since the overturning of Roe v. Wade. They also claim not to be making money by selling user data – instead the funding comes from investors and the premium versions of the apps. The future of period-tracking apps post Roe v. Wade is further analyzed in chapter 6.

6. How can women avoid surveillance post Roe v. Wade – or can they?

Anni Lintula

After the U.S. Supreme Court overturned Roe v. Wade in June 2022, many women's advocates and privacy experts quickly expressed their concerns about period-tracking apps and their potential risks for data privacy. For example, young adult author Jessica Khoury wrote on Twitter: “Delete your period-tracking apps today” (Khoury 2022). The tweet received almost 350,000 likes and 94,000 retweets.

Privacy concerns are not far-fetched because the women who use a period-tracking app share intimate details about themselves, e.g. dates of their periods, weight and the last

time they had sex. In theory, this data combined with the prediction capability of machine learning could reveal that a woman had an abortion, as described in section three.

6.1. Is intimate data safe?

When it comes to data privacy, the period-tracking industry has not proven itself worth users' trust. A popular period-tracking app Flo has been violating its own privacy policy by sharing intimate health details of its users to big tech companies, such as Facebook and Google. The U.S. Federal Trade Commission's (F.T.C.) report indicates that between 2016 and 2019 Flo informed Facebook every time a user logged they were on their period or wanted to get pregnant (Federal Trade Commission 2020). In its privacy policy Flo app had claimed it only shared "non-personally identifiable" information with third parties but this proved false in an investigation done by Wall St. Journal (Schechner & Secada 2022).

Flo is not the only period-tracking application that has failed to protect users' private health data. According to a review published in JMIR, the most popular women's health apps had poor data privacy, sharing, and security standards (Alfawzan, Christen, Spitale & Biller-Andorno 2022). Researchers wrote that "although regulations exist, such as the European Union General Data Protection Regulation, current practices do not follow them" (Alfawzan et al. 2022). The review noted that 20 of the 23 apps analyzed passed on data to third parties, while researchers were unable to determine data protection policies for the other three applications (Alfawzan et al. 2022).

Hence it is clear that women need to be concerned about the tech companies collecting and handling intimate data. Next I am going to examine different options on how – or if – women using period-tracking apps can avoid surveillance.

6.2. Switching apps – is one better than another?

After the supreme court's decision, many women did not delete their period-tracking apps but traded them in for new ones in search of better data privacy. Reports show that the top five period-tracking apps in the US did not lose users but instead improved their app store rankings between June 24th and June 30th 2022 (Poli 2022). Two apps, Stardust and Clue, made it to the top of the charts on Google Play and App Store (Poli 2022).

Choosing the most secure option has not, however, been clear cut for the users. Many users seem to make a decision about which period-tracking app to use based on a false sense of security. Next I am going to have a closer look at Stardust app and Clue app to evaluate

their safety claims.

After the Supreme Court's decision was released, Stardust app started promoting itself in social media as "a women-owned period tracker founded on a belief in freedom of choice and freedom of privacy" (Stardust 2022). However, an application designed by women did not prove to be safer than the other popular period-tracking apps: US tech media TechCrunch made an investigation about the Stardust app's data privacy, and revealed several problems.

The most worrying thing that emerged in the analysis was that if a user logged into the app using their phone number, Stardust shared the user's phone number with a third party analytics service called Mixpanel (Perez & Whittaker 2022). This leaking data could be used to identify individual users of the app.

One way for users searching for better data security has been switching from US based apps to Europe-based apps. Clue, another application which gained popularity after the court ruling, promoted itself as a safer option because they follow European General Data Protection Regulation law GDPR (Clue 2022e). This law is safer and stricter than the U.S data privacy laws. Another argument in favor of Europe-based apps is that US companies are more easily forced to comply with American authorities and courts' requests. Enforcement is obviously trickier against European companies. However, even though data is being processed by a European company, it does not mean that using a Europe-based app protects users from the courts requesting data from them directly. It is vital for the users to understand that once an individual is identified and their data sought after, there is not much these apps can do to protect a user.

After privacy concerns have arisen the developers of period-tracking apps have been looking for ways to anonymize the user data. In September 2022 period-tracking app Flo released a feature called Anonymous Mode for iOS users (Flo 2022d). The setting seeks to protect intimate data in a number of ways, e.g. encrypting data as it's transferred to Flo's server. In addition, data that can be used to identify someone such as user ID and IP address, is kept apart from data logged into the app (Flo 2022d).

But does the anonymous mode really make user data secure? Data-privacy experts have hinted that the whole term "anonymous" is misleading, since learning algorithms can create re-identification processes which link the anonymised data back to users. From a paper published in Nature, it turns out that numerous anonymous datasets have been released and re-identified (Rocher, Hendrickx & de Montjoye 2019). The researchers said in the paper's abstract: "Our results suggest that even heavily sampled anonymized datasets are unlikely to satisfy the modern standards for anonymization set forth by GDPR (Rocher et al. 2019).

6.3. Is deleting an app a good option?

Upon closer inspection, many of the popular period-tracking apps' advertising slogans and promises turn out to be empty. Without a deep analysis of each period-tracking app's privacy policy and carefully performed testing of each app's security protections, it's hard for users to choose one period-tracking app over another. This raises a question of whether users should delete period-tracking apps all together to avoid risking their intimate data.

Under European data privacy law GDPR, data controllers and processors are obliged to return or delete all personal data after the end of services (GDPR 2018). However, not all the applications delete user's data immediately after the application has been deleted. For example Flo states in their privacy policy that when deleting their app, they "retain your personal data for a period of 3 years in case you decide to re-activate" (Flo 2022e).

It is also important to note that period-tracking apps are not the only apps that could be used against women when it comes to criminal prosecution. Search engine history,or a text message to a friend could be as well used to connect someone to an abortion. Even if a woman is sitting in the waiting room of an abortion clinic and scrolling social media on her phone, the app might collect location data. Therefore it seems that period-tracking apps are just a needle in a haystack when it comes to data security.

7. How to build a better future for women and Femtech

Sini-Marja Ant-Wuorinen

Whereas period-tracking should make a person's everyday life easier and increase knowledge about one's health, the consequences after the Supreme Court's overturning Roe v. Wade will comprehensively affect American society and business, not least in the context of Femtech.

President Biden issued an executive order (White House, 2022) to fortify data privacy regarding sensitive data related to reproductive healthcare, yet still many consumers suspect their data will be sold on to third parties or their personal health data could be turned over to law enforcement, in case of subpoena.

What the future holds for Femtech, relies besides on legal matters, tech companies, app developers, investors and not least on the reliability and data safety.. This article cannot take a stand on all of this, let alone predict the future, but in the following we have assessed some of the threats and scenarios for Femtech, based on previous research related to the

topic.

7.1. The struggle is regulation?

The United States, in contrast to GDPR in Europe, does not have a singular law that covers the privacy of all types of data. Instead, it has a mix of laws designed to target only specific types of data in special circumstances. (Klosowski, 2022.)

The regulatory sphere in which Femtech operates fundamentally fails to ensure that the health and safety of femtech users are protected as the market continues to expand (Scatterday, 2021). The U.S. Food and Drug Administration (FDA) currently regulates only *certain* Femtech apps under *full* regulation. However, FDA has already reacted to the need for stricter regulation and created a new category of medical devices subject to regulatory control, *Software Applications for Contraception* (SAC). The category includes e.g. Natural Cycles, which received FDA's approval already in 2018. This indicates it could be possible to bring reproductivity related apps within the scope of better regulation as Taylor (2022) suggests.

Many of the Femtech apps give personalized fertility predictions and are advertised and used as contraceptives, meaning that they should fall within the FDA's definition and as Natural Cycles, they should also be subject to full FDA regulation as medical devices. The problem with FDA categorization is, according to Scatterday (2022), that even after receiving *medical device* status, the focus would be on regulating health-technical issues rather than privacy issues.

In the United States, health information is governed by the Health Insurance Portability and Accountability Act (HIPAA). It was enacted in 1996 in response to patients' inherent privacy concerns following the medical care industry's digitization of medical records. (Gillman 2021.) Reproductive health data shared or obtained outside a *medical setting*, is currently shielded neither by HIPAA federal law nor state consumer protection law. This means that information shared with period trackers, obtained by data brokers, or collected by "unethical crisis pregnancy centers" can be obtained by warrant, court order or subpoena. (Scatterday, 2022). Due to this, healthcare- and legal experts and researchers suggest privacy protections to cover data collected by Femtech apps under HIPAA. If HIPAA were amended to include Femtech apps as *covered entities* which include doctors, hospitals and pharmacies, user data would be protected under HIPAA's Privacy Rule, Security Rule, and Breach Notification Rule (Scatterday, 2022).

> *"The HIPAA Rules generally do not protect the privacy or security of your health information when it is accessed through or stored on your personal cell phones or tablets. The HIPAA rules apply only when PHI (Protected Health Information) is created, received, maintained, or transmitted by covered entities and business associates."* (U.S. Department of Health & Human Services, 2022.)

HIPAA's *covered entity* should in Scatterday´s notion include any app that collects and stores data about users' reproductive health. She suggests *data encryption* to be a reasonable measure for femtech apps to implement, considering the intimate nature of the data collected and the risks involved with possible data breaches.

To ensure that Femtech app providers are held to higher standards, these companies must be regulated. Likewise, Femtech mobile application users need adequate legal protection to rely on when companies fail to protect their personal health information (Rosas, 2019). Also state legislators are addressing the array of privacy issues arising from online platforms. New privacy laws are considered as a solution to obtain better privacy protection. According to NCSL National Conference of State Legislatures (NCSL 2022) certain states, e.g. California, Colorado, Connecticut, Virginia, and Utah have started to address this gap in their comprehensive privacy laws.

7.2. A Critical Feminist perspective and cyber security

The regulatory ambiguities presented in the previous chapters undoubtedly affect what start-ups want to develop and investors fund in the future.

It is clear that in times of uncertainty the development of women's health services are at risk. If consumers start to think reproductive health data can be used against them, they are simply going to stop entering information into the apps. This leads to fewer data to be collected, shared and thus diminishing overall knowledge of women's health.

Studies have shown that the majority of femtech start-ups are led by women. According to McKinsey's survey (2022) Femtech is powered to a significant extent by female entrepreneurs, more than 70 percent of Femtech companies in the analysis had at least one female founder. However, technologies behind start-ups are predominantly funded by men (McKinsey, 2022). This leads to the fact that power in terms of what does and does not get funded, are in the hands of those who do not necessarily use the technology or have an experiential understanding of the reasons why one might want to use it.

An interesting perspective and a critical approach when considering the future of

femtech is called *data* feminism. A book *Datafeminsm* (D'Ignazio, Klein, 2021) provides strategies for data scientists seeking to learn how feminism can help them work for justice, and for feminists who want to work in the expanding field of data science. D'Ignazio and Klein consider how data science can be used to reinforce existing inequalities. They also bring up concerns about the decreasing representation of women among programmers and data architects.

A critical perspective also applies to the interface between health and business. Femtech users must be protected where private industry and health meet because in capitalism profit often comes before rights and interests (McMillan 2022). Growing concerns have already forced Apple, Google, Meta and other tech giants to take steps to rein in the sale of consumer data. Apple recently launched its own App Tracking Transparency feature, that allows iPhone and iPad users to block apps from tracking them (MacWorld, 2021).

Cyber security experts rely on the role of technology in securing data privacy. Developed data encryption *can already* preserve the privacy of both the data and the analysis being conducted on the data. This includes *homomorphic encryption*, which allows firms to perform computations on encrypted data without ever decrypting it and, therefore, without revealing anything sensitive. This means they can share and analyze sensitive data without revealing the underlying information and stay within regulatory requirements. (Hughes, 2022.) As the law enforcement actions protecting consumers' digital health-relevant data are increasing, software developers should also be familiar with privacy and security requirements to adequately address privacy concerns and expectations and practices for future compliance.

8. Conclusions

In this paper we aimed to analyze from various perspectives whether period-tracking applications could be used to target and even punish women seeking abortion in the US after the overturning of Roe v. Wade.

First, we found that critical understanding of period-tracking applications relates to ***recent societal developments*** in the US: restricted abortion rights of post Roe era, user-generated data becoming a possible commodity, and data-related criminal investigation methods of the US law enforcement becoming less transparent and mass-oriented.

We discovered that even though ***Femtech*** has been marketing itself as an empowering

tool, the opposite can be argued. Period-tracking applications such as Flo and Clue claim to be committed to data security, but they have been caught deceiving their users. Femtech also lacks regulation and ethical standards such as those of the medical field. Therefore, data in the wrong hands could pose a threat in the post Roe era of abortion rights.

Moreover, we found that although period-tracking applications are marketed to women as means of ***being in control,*** they were working in opposing ways. Firstly, their ability to help in conceiving or in preventing pregnancies has been questioned. Second, the intimate data collected by the applications has been shared with third parties in many instances, as different studies demonstrate. At the discourse level, the applications may strengthen pre-existing ideas of womanhood and women's sexuality.

When analyzing the period-tracking applications from the perspective of technological and data protocol level, we found that many period-tracking apps have ***poor data privacy*** and security standards. We also discovered that we cannot rule out the possibility that ***machine learning*** could detect or predict abortion from relatively simple input data. Considering this, it seems that we are incapable of reliably assessing what kind of data would be safe to share in period-tracking apps in terms of detecting or predicting pregnancy, or abortion.

With all these developments considered, we argue that it can be legitimately claimed that period-tracking apps could be used against women seeking an abortion in the US.

To draw wider lessons for the future, we argue that the development of the industry is at risk if neither users nor investors believe in its security. As the regulation is currently a confusing and siloed regime and the administration and categories have deficiencies and ambiguities, we suggest that Femtech ***regulation should be more consistent and always aim to protect the individual's data privacy***. Further studies from various perspectives would also be required to fully understand the current state and the possible future developments of this issue.

References

Alfawzan N., Christen M., Spitale G., & Biller-Andorno N. (2022). Privacy, Data Sharing, and Data Security Policies of Women's mHealth Apps: Scoping Review and Content Analysis. *JMIR Mhealth Uhealth*, *10*(5). https://mhealth.jmir.org/2022/5/e33735

Amelang, K. (2022). (Not) Safe to Use: Insecurities in Everyday Data Practices with Period-Tracking Apps. In A. Hepp, J. Jarke, & L. Kramp, *New Perspectives in Critical Data Studies: The Ambivalences of Data Power*, pp. 297–32. Palgrave Macmillan. https://link.springer.com/book/10.1007/978-3-030-96180-0

Atkins C. & Li, D. K. (2022, June 27). Louisiana and Utah trigger laws banning abortions temporarily blocked by courts. *NBC News*. https://www.nbcnews.com/news/amp/rcna35528

Bankmycell. (2022). *How many cellphones are there in the world?* https://www.bankmycell.com/blog/how-many-phones-are-in-the-world

Boulanin, V. (2019). The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk. *Stockholm International Peace Research Institute*, pp. 13-25. https://www.sipri.org/publications/2019/other-publications/impact-artificial-intelligence-strategic-stability-and-nuclear-risk-volume-i-euro-atlantic on 24 Oct 2022

Best, K. (2010). Living in the control society: Surveillance, users and digital screen technologies. *International Journal of Cultural Studies, 13*(1), pp. 5–24. https://doi.org/10.1177/1367877909348536

Bossewitch, J. & Sinnreich, A. (2013). The end of forgetting: Strategic agency beyond the panopticon. *New Media & Society, 15*(2), pp. 224–242. https://doi.org/10.1177/1461444812451565

Center for Reproductive Rights. (n.d.) *After Roe Fell: Abortion Laws By State. Center For Reproductive Rights*. https://reproductiverights.org/maps/abortion-laws-by-state/

Clue. (2022a). *About Clue*. Accessed: October 17, 2022. https://helloclue.com/about-clue

Clue. (2022b). *Clue Plus – Million experiences. One app*. Accessed: October 17, 2022. https://helloclue.com/clue-plus

Clue. (2022c). *Coming soon to the United States of America – Clue Birth Control*. Accessed: October 17, 2022. https://helloclue.com/clue-birth-control-digital-contraceptive-app

Clue. (2022d). *Revolutionize your relationship with Clue Connect*. Accessed: October 17, 2022. https://helloclue.com/articles/about-clue/revolutionize-your-relationship-with-clue-connect

Clue. (2022e). *Patient Data Privacy at Clue: A statement from the CoCEOs.* Accessed: October 26, 2022. https://helloclue.com/articles/about-clue/patient-data-privacy-at-clue-a-statement-from-the-co-ceos

Cole, S. (2022, June 27). The #1 Period Tracker on the App Store Will Hand Over Data Without a Warrant [UPDATED]. *Vice*. Accessed: November 3, 2022. https://www.vice.com/en/article/y3pgvg/the-1-period-tracker-on-the-app-store-will-hand-over-data-without-a-warrant

Diamant, J. & Mohamed, B. (2022). What the data says about abortion in the U.S. *Pew Research Center*. https://www.pewresearch.org/fact-tank/2022/06/24/what-the-data-says-about-abortion-in-the-u-s-2/

Digital Defence Fund. (2022). *Keep Your Abortion Private and Secure*. https://digitaldefensefund.org/ddf-guides/abortion-privacy

D'ignazio, C. & Klein, L. F. (2020). *Data Feminism*. MIT Press.

The Economist. (2019). *Companies should take Californias new data privacy law seriously*. Accessed: October 28, 2022. https://www.economist.com/business/2019/12/18/companies-should-take-californias-new-data-privacy-law-seriously?utm_medium=cpc.adword.pd&utm_source=google&ppccampaignID=17210591673&ppcadID=&utm_campaign=a.22brand_pmax&utm_content=conversion.direct-response.anonymous&gclid=Cj0KCQjwwfiaBhC7ARIsAGvcPe5U5lZibkdSVXY7NZMjjs_F8oJ8j3TrliEDINaXPMLeZ4Q5rDUND0saArs3EALw_wcB&gclsrc=aw.ds

Dobbs v. Jackson Women's Health Organization (2022). Legal Information Institute. *Cornell Law School.* https://www.law.cornell.edu/wex/dobbs_v._jackson_women%27s_health_organization_%282022%29

Duane, M., Contreras, A., Jensen, E. T., & White, A. (2016). The Performance of Fertility Awareness-based Method Apps Marketed to Avoid Pregnancy. *The Journal of the American Board of Family Medicine*, *29*(4), pp. 508–511. https://doi.org/10.3122/jabfm.2016.04.160022

Federal Trade Commission. (2020). *In the Matter of Flo Health, Inc.* Accessed: October 26, 2022. https://www.ftc.gov/system/files/documents/cases/flo_health_complaint.pdf

Flo. (2022a). *Analyzing your cycles and symptoms*. Accessed: October 17, 2022. https://help.flo.health/hc/en-us/articles/4407228784276-Analyzing-your-cycles-and-symptoms

Flo. (2022b). *Flo Milestones*. Accessed: October 17, 2022. https://flo.health/about-

flo/milestones

Flo. (2022c.) *What is included in Flo Premium?* Accessed: October 17, 2022. https://help.flo.health/hc/en-us/articles/360042141812

Flo. (2022d). *Flo, the Leading Female Health App, Launches 'Anonymous Mode'.* Accessed: October 26, 2022. https://flo.health/press-center/flo-launches-anonymous-mode

Flo. (2022e). *Privacy Policy*. Accessed: October 26, 2022. https://flo.health/privacy-policy

Fox, C. A. & Manis, E. (2022): Pregnancy Panopticon. Abortion Surveillance After Roe. *Stop. Surveillance Technology Oversight Project*. https://www.stopspying.org/pregnancy-panoptico

Freis, A., Freundl-Schütt, T., Wallwiener, L.-M., Baur, S., Strowitzki, T., Freundl, G., & Frank-Herrmann, P. (2018). Plausibility of Menstrual Cycle Apps Claiming to Support Conception. *Frontiers in Public Health, 6*, pp. 98. https://doi.org/10.3389/fpubh.2018.00098

Folkendt, K. (2019, September 5). "So What Is Femtech, Anyways?!". *Femtech Insider*. Accessed October 17, 2022. https://femtechinsider.com/what-is-femtech/

Fowler L. R. & Ulrich, M. R. (2022). Femtechnodystopia. *Standford Law Review*, forthcoming 2023. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4099764

Future Market Insights. (2022). Women Digital Health Solutions Market Outlook (2022-2032). *Women Digital Health Solutions Market*. Accessed: October 18, 2022. https://www.futuremarketinsights.com/reports/women-digital-health-solutions-market

Gilman, M.E. (2021). Periods for profit and the rise of menstrual surveillance. *Columbia Journal of Gender & Law, 41*, pp. 100-113. https://heinonline.org/HOL/P?h=hein.journals/coljgl41&i=118

GRPR. (2018). *Right to erasure ('right to be forgotten')*. Accessed: October 26, 2022. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e2606-1-1

Guariglia, M. (2022): What is Fog Data Science? Why is the Surveillance Company so Dangerous? *Electronic Frontier Foundation*. https://www.eff.org/deeplinks/2022/06/what-fog-data-science-why-surveillance-company-so-dangerous

Halpern, S. (2014). The Creepy New Wave of the Internet. *The New York Review of Books*. http://www.nybooks.com/articles/2014/11/20/creepy-new-wave-internet/

Health Apps and Information Survey September 2019. (2019). *Henry J Kaiser Family Foundation*. https://files.kff.org/attachment/Topline-Health-Apps-and-Information-Survey-September-2019

Hendl, T. & Jansky, B. (2022). Tales of self-empowerment through digital health technologies: a closer look at 'Femtech'. *Review of Social Economy, 80*(1), pp. 29-57. https://doi-org.ezproxy.utu.fi/10.1080/00346764.2021.2018027

Hildebrandt, M. (2016). The New Imbroglio – Living with Machine Algorithms. In: L. Janssens (Hg.), *The Art of Ethics in the Information Society*, pp. 55–60. Amsterdam University Press. https://doi.org/10.25969/mediarep/13395

Hughes, M. (2022). Do data regulations properly protect consumers? *World Economic Forum*. Accessed: October 31, 2022. https://www.weforum.org/agenda/2022/08/do-data-regulation-properly-protect-consumers/

Hull, N. E. H. & Hoffer, P. C. (2010). *Roe v. Wade: The abortion rights controversy in American history*. University Press of Kansas.

Joffe, C. E., Weitz, T. A., & Stacey, C. L. (2004). Uneasy allies: pro-choice physicians, feminist health activists and the struggle for abortion rights. *Sociology of Health & Illness*, *26*(6), pp. 775-796. https://doi.org/10.1111/j.0141-9889.2004.00418.x

Khoury, J. (2022, June 24). Tweet. Accessed: Octobre 26, 2022. https://twitter.com/jkbibliophile/status/1540345161955385345

Klosowsky, T. (2022). The State of Consumer Data Privacy Laws in the US. *The New York Times*. https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/

Lupton, D. (2012). M-health and health promotion: The digital cyborg and surveillance society. *Social Theory & Health*, *10*(3), pp. 229–244. https://doi.org/10.1057/sth.2012.6

Lupton, D. (2015). Quantified sex: A critical analysis of sexual and reproductive self-tracking using apps. *Culture, Health & Sexuality, 17*(4), pp. 440–453. https://doi.org/10.1080/13691058.2014.920528

Macworld. (2021). *What is App Tracking Transparency and how do you block app tracking?* Accessed: October 30, 2022. https://www.macworld.com/article/344420/app-tracking-transparency-privacy-ad-tracking-iphone-ipad-how-to-change-settings.html

Majeed, Z. (2022). US Law Enforcement Purchases Data From Third Party Firm To Spy On Americans: Report. *RepublicWorld.com.* https://www.republicworld.com/world-news/us-news/us-law-enforcement-purchases-data-from-third-party-firm-to-spy-on-americans-report-articleshow.html

McMillan, C. (2022). Monitoring female fertility through 'Femtech': The need for a whole-system approach to regulation. *Medical Law Review*, *30*(3), pp. 410-433. Accessed: October 30, 2022. https://doi.org/10.1093/medlaw/fwac006

McKinsey & Company. (2022, February 14). *The dawn of the FemTech revolution*. Accessed: October 30, 2022. https://www.mckinsey.com/industries/healthcare-systems-and-services/our-insights/the-dawn-of-the-femtech-revolution

Mishra, P. & Suresh, Y. (2021). Datafied body projects in India: Femtech and the rise of reproductive surveillance in the digital era. *Asian Journal of Women's Studies, 27*(4), pp. 597-606. https://doi.org/10.1080/12259276.2021.2002010

NCSL National Conference of State Legislatures. (2022). *2022 Consumer Privacy Legislation*. Accessed: October 31, 2022. https://www.ncsl.org/research/telecommunications-and-information-technology/2022-consumer-privacy-legislation.aspx

Neff, G. & Nafus, D. (2016). *Self-Tracking*. MIT Press.

Nicas, J. (2021). What Data About You Can the Government Get From Big Tech? *New York Times*. https://www.nytimes.com/2021/06/14/technology/personal-data-apple-google-facebook.html

Perez, C.C. (2019). *Invisible Women: Data Bias in a World Designed for Men*. Abrams Press.

Perez, S. & Whittaker, Z. (2022, June 27). *Period tracker Stardust surges following Roe reversal, but its privacy claims aren't airtight.* Accessed: October 26, 2022. https://techcrunch.com/2022/06/27/stardust-period-tracker-phone-number/

Petronzio, M. (2014, April 26). How One Woman Hid Her Pregnancy From Big Data. *Mashable*. https://mashable.com/archive/big-data-pregnancy

Poli, K. (2022, July 20). *The Most Popular Period-Tracking Apps, Ranked by Data Privacy.* Accessed: October 26, 2022. https://www.wired.com/story/period-tracking-apps-flo-clue-stardust-ranked-data-privacy/

Popli N. & Bergengruen V. (2022, July 1). Lawmakers Scramble to Reform Digital Privacy After Roe Reversal. *Time*. https://time.com/6193224/abortion-privacy-data-reform/

Privacy International. (2019, September 9). *No Body's Business But Mine: How Menstruation Apps Are Sharing Your Data*. Accessed: October 28, 2022. http://privacyinternational.org/long-read/3196/no-bodys-business-mine-how-menstruations-apps-are-sharing-your-data

Privacy International (2022, July 22). *Privacy and Sexual and Reproductive Health in the Post-Roe world*. Accessed: November 3, 2022. http://privacyinternational.org/long-read/4937/privacy-and-sexual-and-reproductive-health-post-roe-world

Rocher, L., Hendrickx, J.M., & de Montjoye, YA. (2019). *Estimating the success of re-identifications in incomplete datasets using generative models*. Accessed: October 26, 2022. https://www.nature.com/articles/s41467-019-10933-3

Rosas, C. (2019). The future is femtech: Privacy and data security issues surrounding femtech applications. *Hastings Bus. LJ*, *15*, pp. 319.

Ruckenstein, M. (2014). Visualized and Interacted Life: Personal Analytics and Engagements with Data Doubles. *Societies, 4*(1), pp. 68–84. https://doi.org/10.3390/soc4010068

Scatterday, A. (2021). 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*, pp. 636. https://heinonline.org/HOL/P?h=hein.journals/ncjl23&i=659.

Schechner S., Secada, M. (2022, 22 February). *You Give Apps Sensitive Personal Information. Then They Tell Facebook. The Wall Street Journal*. Accessed: October 26, 2022. https://www.wsj.com/articles/you-give-apps-sensitive-personal-information-then-they-tell-facebook-11550851636

Sherman, J. (2021, August 23). Data Brokers Know Where You Are—and Want to Sell That Intel. *Wired*. https://www.wired.com/story/opinion-data-brokers-know-where-you-are-and-want-to-sell-that-intel/

Singer, N. (2012, June 16). "Acxiom, the Quiet Giant of Consumer Database Marketing". *The New York Times*. https://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html

Sneed, T. (2022, June 28). Abortion can resume at some Texas clinics after court blocks pre-Roe ban. *CNN Politics*. https://edition.cnn.com/2022/06/28/politics/texas-abortion/index.html

Taylor, A M. (2021). Fertile ground: rethinking regulatory standards for femtech. *UC Davis Law Review, 54*(4), pp. 2267-2300. https://heinonline.org/HOL/P?h=hein.journals/davlr54&i=2279

The Associated Press (2022). Google says it will erase U.S. user data about trips to abortion clinics. *CBC/Radio-Canada.* https://www.cbc.ca/news/world/google-data-abortion-clinics-1.6508856

The White House. (2022). *President Biden to Sign Executive Order Protecting Access to Reproductive Health Care Services*. Accessed: October 29, 2022. https://www.whitehouse.gov/briefing-room/statements-releases/2022/07/08/fact-sheet-president-biden-to-sign-executive-order-protecting-access-to-reproductive-health-care-services/

Thomas, G. M., & Lupton, D. (2015). Threats and thrills: pregnancy apps, risk and consumption. *Health, Risk Society, 17*(7-8), pp. 495–509. https://www.academia.edu/49719960/Threats_and_thrills_pregnancy_apps_risk_and_consumption

Verhelst, H. M., Stannat, A. W., & Mecacci, G. (2020). Machine Learning Against Terrorism: How Big Data Collection and Analysis Influences the Privacy-Security Dilemma. *Science and engineering ethics*, *26*(6), pp. 2975-2984. https://doi.org/10.1007/s11948-020-00254-w

Väntönen, E. (2022). Tämä on minun päätökseni. *Helsingin Sanomat*. https://www.hs.fi/ulkomaat/art-2000009126561.html?share=afbf9f46b611d195de1154752fa3417f

Walker, K (2021): It's time for more transparency around government data demands. *The Keyword*. https://blog.google/outreach-initiatives/public-policy/its-time-for-more-transparency-around-government-data-demands/

Walker, K. (2021). The urgent necessity of enacting a national privacy law. *The Keyword*. https://blog.google/outreach-initiatives/public-policy/the-urgent-necessity-of-enacting-a-national-privacy-law/

Warren, Wyden, Murray, Whitehouse, Sanders Introduce Legislation to Ban Data Brokers from Selling Americans' Location and Health Data. (2022, June 15). Newsroom/Press releases. *Elizabeth Warren*. https://www.warren.senate.gov/newsroom/press-releases/warren-wyden-murray-whitehouse-sanders-introduce-legislation-to-ban-data-brokers-from-selling-americans-location-and-health-data