Unfinished Business:
Incorporating a Gender Perspective into Digital Advertising Reform in the UK and EU.

Lucy Purdon
Senior Tech Policy Fellow at Mozilla Foundation

October 2023

Contents

Methodology

This report and its associated products are the outcome of a 12-month Mozilla Fellowship that ran from January 2023 to January 2024. The project strives to include the experiences of cis- and transgender women as well as those assigned “female at birth” in the United Kingdom (UK) and the European Union (EU). The project incorporates desk research; an online consumer survey of 1,000 FemTech (female technology) users in the UK; a survey of 48 FemTech C-suite and marketing executives and investors; expert interviews, and three industry roundtable discussions. Thank you to everyone who participated in the making of this report and in particular all the women who shared their stories with me.

Credits

Supported by moz://a
This study was made possible through a Mozilla Fellowship.

Thanks to Anna Butterworth from Ultra Violet Agency,
Harriet Kingaby at the Conscious Advertising Network (CAN)
and the team at Mozilla Foundation.

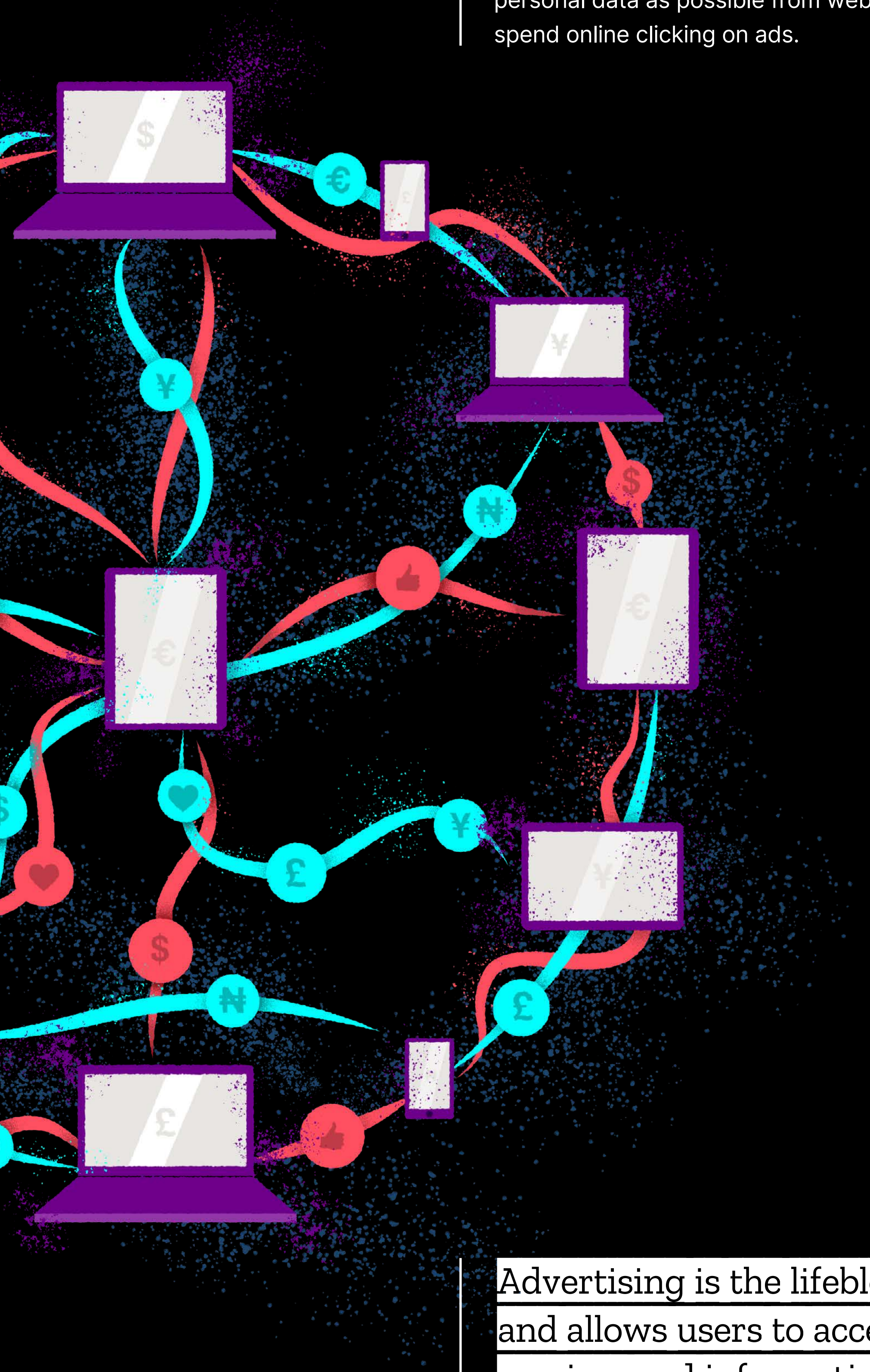
Design and illustration by Working Progress.

Chapter One: Introduction

As the UK headed into a third national Covid-19 lockdown in January 2021, the UK government ran a social media campaign with a series of adverts urging people to “Stay Home. Save Lives.”[1] The illustration featured households where a man reclined on a sofa while women looked after the baby, home schooled the children and did the housework. It had more in common with adverts from the 1950s than the 2020s and was swiftly withdrawn.

Communities around the world are experiencing a backlash against women’s rights,[2] exacerbated by the Covid-19 pandemic. Hard won progress for women’s rights in the home, workplace, healthcare settings, andonline are being rolled back. Women are disproportionately impacted by gender-based violence, especially the lesbian, gay, bisexual, transgender (LGBT) + community, women of colour, and women with disabilities.[3] Women’s healthcare is underfunded and under researched.[4] Women’s autonomy over their own bodies is a battleground, especially when it comes to reproductive rights.

Turning to technology and the internet is second nature to many people looking to find safety, escape, information, and support. The internet is built on advertising revenues, which often depend on collecting as much personal data as possible from web users to maximise the time users spend online clicking on ads.



> Advertising is the lifeblood of the internet and allows users to access a wide range of services and information in exchange for their attention or data.

The UK is the largest digital advertising market in Europe. In 2022, £26 billion was spent on digital advertising in the UK.[5]

This lucrative advertising business model has given rise to an extremely complex and opaque industry where collecting and monetising personal data has become extractive and exploitative, while remaining largely hidden from view.

> For internet users, the reality is that going online means being tracked for advertising.[6]

Permissions for the collection and use of data are buried in so many clicked-accept-but-didn't-read privacy policies. Policymakers and regulators globally are picking up the pieces from the decision in the 1990s to leave tech companies essentially unregulated to encourage innovation.

This study is written from the perspective of a privacy advocate and is not a technical study of "AdTech" — a catch-all term that describes the tools used to target, deliver, and measure the performance of digital advertising. Civil society experts have worked tirelessly to chip away at the complexity and opaqueness of the digital advertising industry, pursuing regulatory action for privacy violations that have often resulted in eye-watering fines. Thanks to these advocates, who have published technical explanations of this complex process, the intrusive nature of AdTech and data broker operations are well documented: the harms to privacy, the discrimination, the fraud, the scams, the disinformation funding, and ultimately the likelihood that targeted advertising might not be as effective as claimed.[7]

Inspired by a feminist research methodology,[8] this study is about the women behind the data, the impact of the misuse of women's personal data and the importance of applying a gender perspective to better protect it.

The primary audience for this study is policymakers in the UK and EU working on digital advertising reform. The study advocates for incorporating a gender perspective into reforms and analyses reform proposals in the UK and EU through this lens, with the goal of protecting women's privacy. While gender mainstreaming is not a new concept in policy making, more attention on tech policy is needed in upcoming digital advertising reforms, which will also feed into the development of policy and regulation around artificial intelligence (AI).

It is no coincidence that the biggest players in digital advertising are also the ones forging ahead with AI, powered by the data they are amassing.

In addition, by engaging with the booming FemTech industry throughout the project, this study documents the seeds of innovative alternatives that could transform digital advertising into something more enjoyable and less intrusive, while preventing valuable data on women's health being exploited. The findings are summarised at the end of the study along with recommendations for policymakers and for the FemTech industry moving forward.

Advertising is **not going away.**

Women may want to find out about new products, but they don't want to pay a high price in terms of their privacy.

It's that simple.

This study intends to contribute to the movement spurring a cultural shift to reframe our relationship with tech companies and serve as a catalyst for change.

*Policies that help **women** help **everyone.***
We demand better.

Chapter Two: Healthcare and Technology: The Birth of FemTech

While astronaut Dr. Sally Ride, the first woman in space, was training for her role as a Mission Specialist on board the Space Shuttle *Challenger* in 1983,[9] National Aeronautics and Space Administration (NASA) engineers were puzzled over how many tampons a woman would need for a one-week flight. They asked Sally, "would 100 be enough?" "No," Sally patiently responded, "that would not be the right number."[10]

Women's bodies have presented a mystery to science and to medicine since the practice began. The male body was perceived in medicine as the "default standard," which has had major repercussions for women's health and safety over the years. In *Invisible Women: Exposing Data Bias in a World Designed for Men*, Caroline Criado Perez presents examples where a woman's place in the world is consistently overlooked:

"Routinely forgetting to include the female body in design – whether medical, technological or architectural – has led to a world that is less hospitable and more dangerous for women to navigate. It leads to us injuring ourselves in jobs and cars that weren't designed for our bodies. It leads to us dying from drugs that don't work. It has led to the creation of a world where women just don't fit very well."

Women's healthcare is notoriously underfunded and under researched, resulting in a gender health gap.[11] In the UK, women receive poorer healthcare than men when it comes to diagnosis of heart attacks[12] and cancers.[13] The view is even worse through an intersectional lens: a 2021 study revealed that women of colour are four times more likely to die in childbirth than white women in the UK.[14] The UK's National Health Service (NHS) reports LGBTQ+ individuals face barriers and discrimination when accessing healthcare.[15] One hundred percent of women will go through the menopause, and yet the experience is poorly understood or researched. Endometriosis can take up to eight years to diagnose.[16] Gynaecology waiting lists have grown by over 60% across the UK since the start of the Covid-19 pandemic.[17]

The 2023 World Economic Forum (WEF) identified investment in improving women's health as vital to creating a "healthier, more equitable world for all" and estimated that a $300 million investment in research for better female health could improve both direct healthcare economics and indirect productivity costs, leading to a return of $13 billion.[18]

> It is understandable that women are increasingly taking matters into their own hands and turning to technology to seek information, manage and improve their health, wellness, and sexual pleasure.

A reluctance to talk about sex and menstruation in society means many women rely on the internet for health advice and management. Products collectively known as "FemTech" are helping to open the conversation about women's health and break barriers and taboos. According to the *2022 FemHealth Insights* report, 60% of FemTech startups were founded in the last five years.[19] However, the FemTech industry faces many challenges and obstacles to growth. Despite the various estimates of FemTech industry growth — set to be worth over $100 billion globally by 2030 according to one forecast[20] — there is a twofold lack of funding. First, the women's healthcare tech sector is underfunded and under-researched to begin with.[21] Second, only a fraction of investment goes to companies with female founders, who make up the vast majority of FemTech companies. The British Business Bank reported that out of every £1 of venture capital investment, all-female founder teams in the UK get less than 1p.[22]

FemTech clearly has an important role to play in empowering women to take control of their own health while also improving data collection to enable further research into under-researched conditions and thereby improve outcomes.

Healthcare professionals approve of FemTech innovations. The *2022 UK Women's Health Strategy for England*, which aims to address gender bias in healthcare, promotes the collaborative use of FemTech:

"FemTech – technologies that specifically focus on women's health-related topics, such as fertility, period tracking, pelvic health and sexual wellness – is a growing area of digital health. These technologies can empower women to have fair access to clinically safe technologies – whether diagnostic, therapeutic or preventive – to ultimately improve health outcomes for women. We want to see greater use of digital technologies to empower women by demystifying and simplifying the process for companies to scale and launch their products in the UK."[23]

The rise of FemTech has also opened a new and rich potential data source for the digital advertising industry. In *Fighting for Privacy*, Danielle Keats Citron says that while the corporate tracking of personal data for advertising is mostly equal opportunity, this is not the case when it comes to women's health data, where there is seemingly no end to data collection. In this market, she says, women are 75% more likely than men to use health apps, making them more open to surveillance.[24] Women have more life milestones and "brand capture" life moments such as menstruating and having a baby. Women also experience more moments of specific vulnerability during these life milestones such as seeking fertility treatment, giving birth, managing the menopause. We need to ensure that these moments of vulnerability do not lead to exploitation.

Chapter Three: Where's the Harm? Women's Lived Experience of Privacy and Safety.

In June 2023, while 23-year-old Hannah Smethurst was waiting alone at Abu Dhabi Airport for her flight to Manchester in the UK, she received a WhatsApp message from a man she didn't know: *"Heyyy, I have seen u from abudhabi, [smiling emoji]."* Hannah asked how the sender got her number, he replied: *"I searched u in the system."* Further messages clarified he worked for the airline. After Hannah went silent the last message the man sent was: *"FYI, Ur flight is boarding."*

Paige Lockwell-Burge told the British Broadcasting Corporation (BBC) she received messages from a man who checked her into her hotel room in March 2023, asking if she was single. She said, *"I felt really unsafe, obviously this person not only got my name, but has seen my licence with my address on it…it just puts this horrible feeling in your head."*[25]

Another woman, Brooke, also told the BBC she received unsolicited contact from a hotel receptionist two weeks after her stay. *"Women just want to be left alone,"* she said.[26]

Hannah was so scared at Abu Dhabi Airport she almost didn't board her flight home to Manchester. She told *The Guardian* newspaper *"I was alone, so I just felt really vulnerable because it stuck in my mind that he knows my number, knows my home address and my full name and email address and obviously everything you give the airline when you book,"* she said. *"I just felt vulnerable and scared. [It] made me feel like he knew what was going on and where I was going."*[27]

What happened to these women is obviously frightening, emotionally distressing and crucially, *visible*. These women paid for a service, strangers entrusted with their personal details betrayed that trust and intruded on their lives through creepy unsolicited contact that made them feel unsafe. It is clearly unacceptable behaviour.

Privacy advocates are often met with a shrug when warning about violations of privacy and questioned about the harms of excessive data collection and sharing, which is often not visible. In their 2023 paper, *Sociotechnical Harms of Algorithmic Systems: Scoping a Taxonomy for Harm Reduction*, Shelby et.al explain:

"Privacy violation occurs when technology design leads to diminished privacy, such as enabling the undesirable flow of private information, instilling the feeling of being watched or surveilled, and the collection of data without explicit and informed consent. These violations have also been framed as 'data harms,' which encompass the adverse effects of data that 'impair, injure, or set back a person, entity, or society's interests.'"[28]

Hannah, Paige, and Brooke's experiences are just a snapshot of the importance of the right to privacy and data protection and the connection with personal safety. Maintaining control over personal and intimate information is paramount for women's safety, particularly in situations where they are vulnerable.

The argument presented in this study is that through its design, the digital advertising ecosystem potentially puts women in a perpetual state of vulnerable situations and it is paramount that this is considered by policymakers.

Chapter Four: The Evolution of Digital Advertising and an Industry Stacked Against Women.

"Have you ever clicked your mouse right here? YOU WILL."

In 1994, these pixelated words in multi-coloured neon comprised the first ever banner advert on the internet. Internet advertising caught on at speed and revolutionised the advertising industry. Much has been written about the evolution of the digital advertising industry; this chapter focuses on how that evolution has impacted women.

Google's search engine was launched in 1998. Shoshana Zubhoff recounts Google's early history in detail in *The Age of Surveillance Capitalism*, particularly the way the company steered towards monetising visitors' "behavioural data" for advertising by predicting their behaviour (search terms themselves plus spelling, phrasing, location, click patterns, etc.) She says, *"With Google's unique access to behavioural data, it would be possible to know what a particular individual in a particular time and place was thinking, feeling and doing. That this no longer seems astonishing to us, or perhaps even worthy of note, is evidence of the profound psychic numbing that has inured us to a bold and unprecedented shift in capitalist methods."*[29]

And this is where it gets messy. Call it microtargeting,[30] behavioural targeting, or behavioural surveillance, the experience of going online changed forever.

> Every search, question, like, click, scroll, and spelling mistake sends signals which makes money for some company somewhere.

If Google had digital advertising sewn up due to the behavioural insights through search at the start of the millennium, Facebook entered the game and perfected its monetisation of user data through social media around 2008. As everyone witnessed astronomical multi-billion-dollar annual profits for Google and Facebook, monetising data for advertising became *the* business model of the internet. Platforms like Twitter, YouTube, Instagram, and Pinterest followed suit.

Companies offering search and social are "walled gardens" of data and have a detailed view of user behaviour on their own platforms, which they guard possessively.

When platforms reassure us that they never sell our data, this is not the full story.

The business model is not about selling data, as this is not where the value lies. Rather, the business model is selling you and your attention to advertisers. This is one of the reasons why the 2018 Cambridge Analytica scandal made such an impact and hit Facebook so hard. Cambridge Analytica obtained data on approximately 87 million Facebook users through a third-party app, called This is Your Digital Life, to build profiles of users to target with political ads.[31] Facebook lost control of its most valuable asset, and landed a $5 billion fine from the Federal Trade Commission (FTC) for failing to protect user data.[32]

Although the walled gardens of search and social media still dominate digital advertising, monetising data is lucrative for others. To achieve the detailed, joined-up view enjoyed by the big platforms, an ecosystem has evolved to track consumers across services, browsers, and devices. This gave rise to a complex network of companies that exist to extract valuable personal data and work together to track users and share data to enable targeted advertising. These are the “intermediaries,” such as data brokers and AdTech companies, that sit between the advertisers and the platforms/publishers. As AWO stated in a recent study for the European Commission: *“In the current digital advertising ecosystem, buying and selling ads without the use of personal data is rare.”*[33]

There are many online tracking methods; the best known are third-party cookies. A brand or publisher allows another company to place a “cookie” (a tracker) on their website which captures behaviour on that website and can also follow users around the internet, collecting more information. It is not unusual for users to be asked to accept over 50 cookies when accessing websites — each cookie placed there by a different company, including the big platforms, whose business it is to collect data about what you do online across services, browsers, and platforms. Third-party cookies were the go-to trackers, until Mozilla, Apple and Google announced their browsers would begin to block their use.[34]

The scramble to collect more information from more sources has got out of hand. Sources of online data are anywhere and everywhere, including from “open” sources such as the electoral roll, the census and social media. Meanwhile, products have seemingly been developed with the main goal of collecting data to sell, for example the 2014 Android torch app that collected location data and accessed user contacts.[35]

A well-established trade in personal data is spearheaded by "data brokers" (companies that collect, buy, and sell personal data). Any company could potentially be a data broker if they deem the personal data they collect ("first-party" data) has value. Data brokers can then sell it on to a third party. Many businesses monetise the data they collect on their customers, especially retailers, banks, telcos, and supermarkets. Data could include an individual's name, home or work address, date of birth, marital or family status, education level, income, purchasing history, search and browsing habits, location data, or financial information.

This trade goes on and on, with data being collected from one source, sold to another, and then on to another.

In a 2020 investigation, the UK's Information Commissioner's Office (ICO) mapped the "circular nature" of the trade in personal data and the significance of certain "hubs" in the sector, with data flowing in and out.[36]

The UK's Competition and Markets Authority (CMA) stated in its 2020 *Online Platforms and Digital Advertising Market Study* that "identifying users is crucial to tracking."[37] The goal of tracking for advertising is to link the activity of a single user to build a more complete profile of that user. It is likely that every person has a unique profile that advertisers use to target them, made up of personal data collected, combined, analysed, and inferred. Information and activities are tied to a unique identifier to enable companies to build a profile of individuals' behaviour across the web. Digital identifiers like emails and phone numbers are the common denominator that link profiles across different services, devices, and platforms. People are then labelled or "segmented" into different categories. Researchers recently uncovered 650,000 such labels such as "heavy purchaser of pregnancy test," "likely symptoms of menstrual cramps," "infertility/IVF," "user pregnancy/ovulation apps," "dealing with stress- emotional," "picture perfect families," etc.[38] These profiles are then auctioned off to advertisers in the split second it takes a user to open a web page, in a process called "real time bidding" (RTB).[39]

AdTech companies often argue that the data is anonymised, but there are studies demonstrating that re-identification can happen with just a few data points. One study, *On the Unicity of Smartphone Applications* shows that the list of apps installed by individual smartphone users is "quite unique" and that knowing "any 4 apps installed by a user are enough (more than 95% times [sic]) for the re-identification of the user in our dataset."[40] App download information can reportedly be purchased from data brokers; a 2022 *Motherboard* investigation obtained a list of unique identifiers for devices that had the period tracking app "Clue" installed.[41]

Contains 10,000 women who have:
LOCATION VISITED
Contains 10,000 women who are:
NEUROTICISM
Contains 10,000 women who are dealing with:
DEPRESSION MEDICATION
ADDICTION

Through this complex and vast system of never-ending sources, intimate personal data is collected and combined without our knowledge or consent.

Behaviour is tracked and analysed and assumptions made about a woman's life and therefore, in the context of advertising, what she might buy. For example, a common assumption is that women of a certain age must want a baby (many don't). A common fallacy is that if a woman is pregnant, she will have a healthy baby nine months later (many can sadly say this is not the case). Based on these assumptions and fallacies, women are targeted with, for example, unwanted baby products. On an individual level, targeting in this way risks causing unnecessary feelings of shame and grief. On a societal level, it perpetuates gender norms and reinforces stigma and taboos around discussions of women's bodies that are already deeply rooted in society.

It is important to note that companies might not be "selling" data — some are giving it away. In return they can re-target existing consumers or analyse consumer behaviour for their own purposes. Software development kits (SDKs), used by app developers, tracks a user's interactions with an app and often shares that data with third parties. Similarly, analytics pixels collect data to inform engagement. These "industry standard" tools and their data collection and sharing practices are finally coming under scrutiny, detailed in later chapters.

This process is not just happening in relation to commercial advertising. As researcher Wolfie Christl wrote, *"The pervasive real-time surveillance machine that has been developed for online advertising is rapidly expanding into other fields, from pricing to political communication to credit scoring to risk management."*[42]

Credit reference agencies (CRAs) are one of the biggest purchasers of third-party data (i.e., data they have not collected themselves). People today have no choice but to engage with credit reference agencies if we want to apply for a loan, mortgage, insurance etc. In the UK alone, the ICO noted that *"there is a large, well-established trade in personal data by data brokers, both between themselves and other organisations. It is a complex ecosystem of companies who* [sic] *offer data broking services, ranging from very large multi-national companies to small UK firms. The three large CRAs in the UK – Experian, Equifax and TransUnion – also operate as data brokers. Other companies solely operate as data brokers, while others offer additional data services as well, such as ID verification and anti-money laundering products."*[43]

Back in 1997, the first pop-up ad appeared on the internet. Deemed annoying by almost every internet user, by 2000 most browsers blocked pop-up ads by default. This launched a cat-and-mouse game of adverts and trackers vs. blockers that many in the industry, including Mozilla, are still playing today.

Since the implementation of the General Data Protection Regulation (GDPR), the availability of third-party data in the open market has decreased, but not disappeared. Currently, the European Commission (EC) is nudging relevant stakeholders to come up with voluntary solutions to simplify consumer choices when it comes to accepting cookies.[44] Meanwhile, third-party cookies are being phased out by browser owners including Google, Apple, Microsoft, and Mozilla. Google and Apple have already taken steps to restrict third-party tracking on their platforms by phasing out mobile advertising identifiers (with the unfortunate acronym of MAIDs) and developing more privacy preserving methods for targeting and measuring ad performance on browser and mobile.

However, untangling existing tracking methods is extremely complex. What's more, the industry is addicted to tracking and so is exploring other, potentially even more harmful techniques. Mozilla, for example, has warned about the tracking potential of browser fingerprinting.[45] With this in mind, the phasing out of third-party tracking cookies and MAIDs represents an important opportunity for policymakers and regulators to support innovation in alternative advertising methods.

> Women are at the mercy of who is collecting and interpreting their data and making assumptions about their lives.

Let's say that purchase data obtained from your supermarket loyalty scheme shows you buy nappies. You might be sent a discount voucher. It does not stop there. Assumptions can then be made on your family status, the number of children you have and their ages. It doesn't stop there. When discussing stigmatisation of black women's fertility in the US, Ruha Benjamin asks in *Race after Technology*, *"one may wonder of the consequences of purchasing too many diapers [nappies]. Does reproductive excess lower one's credit? Do assumptions about sex and morality, often fashioned by racist and classist views, shape the interpretation of having children and purchasing diapers?"* She continues: *"In these various scenarios, top-down reproductive policies could give way to a social credit system in which the consequences of low scores are so far-reaching that they could serve as a veritable digital birth control."*[46]

And so it goes on.

The overturning of Roe vs. Wade, which ended the federal protection for abortion in the US, was a lightbulb moment for many of the real life implications of intimate data collection on a woman's safety and the surveillance possible through technology.

Reports abound of women deleting menstruation apps[47] or even avoiding using Google[48] in fear of location tracking, online searches, online shopping habits and suspected missed periods being weaponised and used to prosecute them for seeking an abortion. For women in the 21 countries where abortion has been illegal for years, this fear is already a reality.[49]

The level of granular detail on individuals was built up for the purposes of commercial advertising, but the potential for other uses did not go unnoticed. It is no surprise that the same methods for targeting commercial ads are used to target certain demographics with political messages, or even to discourage some demographics from voting (often in highly charged elections from Trump[50] to Brexit[51] to Kenya.)[52] More recent investigations reveal the goldmine for surveillance presented by the advertising ecosystem and the opportunities for exploitation, including a 2020 *Motherboard* investigation into the US military buying location data from data brokers.[53] As Omer Benjajob writes in a *Haaretz* investigation into Israeli cyber companies developing surveillance capabilities through exploiting the advertising system, *"this isn't an attempt to breach a device via the backdoor, but to allow something to enter it cleverly through a front window, a window that is wide open thanks to the world of advertising that sustains the entire internet economy."*[54]

This chapter presents a simplified version of a complex industry. The core message is this:

Digital advertising does not operate solely on the information people voluntarily give with consent.

This is crucial because the expectation and responsibility is weighted against the individual to manage their own privacy. Women are right to be cautious. Increasingly, they are tricked into sharing intimate data, such as with employers[55] or fertility apps funded by anti-abortion campaigners.[56] In the current climate, we will never gain sufficient knowledge of the ways in which personal data will be extracted, combined, aggregated, and analysed over the years by thousands of organisations going to great lengths to obtain this valuable data.

Chapter Five: Who Cares?

"Many of the rights we thought were secure are not and this is not a problem of certain countries, it's a problem that cuts across the world."

- Susanna Malcorra, GWL Voices.[57]

The extent of a woman's vulnerability to having her intimate data weaponised against her depends on her situation and where she lives. Maryam Mehrnezhad and Teresa Almeida call this variance "differential vulnerabilities," a theme that appears on several occasions in this study.[58]

A trope often repeated by interested parties is that privacy is dead and people simply do not care about their data. Indeed, people express concern about privacy but often don't act on it – a phenomenon known as the "privacy paradox".[59] This paradox raises dilemmas for policymakers who are continually trying to prioritise resources and solutions for the most salient societal problems.

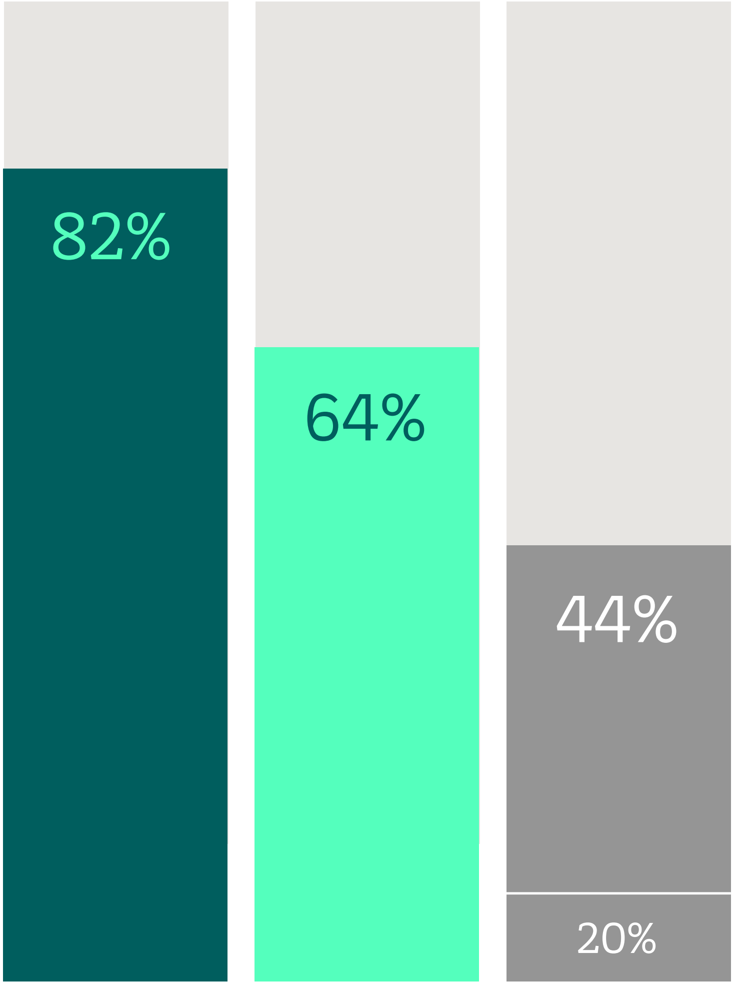
There are many studies on public attitudes to data sharing, but few focus exclusively on women.

In studies that do focus on the gender differences when it comes to managing privacy online, women tend to show greater awareness of the uses of data.

For example, in their 2014 study, Mark Rowan and Josh Delinger outlined how women are more concerned than men if the exact location of their smartphone is shared with third parties and disable location tracking more often than men.[60]

The ICO recently launched a review of period trackers following the results of a poll revealing over half had concerns about the security of the data they share and how it is used. According to the ICO: *"The research also showed over half of people who use the apps believed they had noticed an increase in baby or fertility-related adverts since signing up. While some found the adverts positive, 17% described receiving these adverts as distressing."*[61]

As part of the methodology for this Mozilla Fellowship project, an independent survey was conducted of 1,000 women in the UK who identify as using FemTech on their attitudes towards data collection and sharing.[62]



82%
felt it is not clear and transparent when using FemTech apps what personal data is collected and how it is used.

64%
had concerns about personal information being shared with third parties.

44%
said they had deleted an app because of privacy concerns. Of those that specified the app, 20% identified it as a period or fertility tracking app.

> There is clearly a need to listen more closely to women's concerns around data collection and sharing as it relates to their safety and wellbeing.

And women will respond when asked: Nearly 100,000 in England alone responded to the UK government's survey on women's health as part of the consultation to inform the *Women's Health Strategy*.[63]

Chapter Six: Reframing Our Relationship with Tech Companies: A Gender Perspective in Policymaking and Regulation.

“I propose a literal dick measuring contest 📏 ”

- @elonmusk, 10th July 2023.

The kind of macho energy on display when Elon Musk and Mark Zuckerberg, two of the richest Silicon Valley CEOs, publicly challenged each other to a cage fight and other activities in the summer of 2023[64] shows up in design and decision making across the sector. Advertising veteran Cindy Gallop said in 2019, *“The young white male founders of the tech platforms that dominate our lives today are not the primary targets of harassment, abuse, sexual assault, violence, and rape — so they don’t proactively design for it.”*[65] Many (female) AI researchers have sounded the alarm over concerns that AI models reflect existing biases, with an outsized impact on women and marginalised communities.[66]

In considering much needed regulation for the tech sector, significant attention must be paid to a gender perspective and incorporation of different voices to avoid negative impacts and harms, not just as a result of biased or unbalanced training data but also in system design from the start.

The theme of the United Nations International Women’s Day in 2023 *“DigitALL: Innovation and technology for gender equality”*, provides an excellent starting point for reforms. Central to the UN’s efforts is a commitment by member states at the 67th session of the Commission on the Status of Women (CSW67) to mainstream a gender perspective into digital policies to remove barriers to participation and in the design of emerging technologies. The agreed conclusions adopted by member states includes a commitment to, *“adopt regulations to ensure they are subject to adequate safeguards to combat new risks, gender stereotypes and negative social norms, data privacy breaches and improve transparency and accountability.”*[67]

A lack of gender analysis in many areas of policy is becoming obvious, from the burden of unpaid care work falling predominantly on women, gaps in healthcare and the cost of childcare to treatment in the workplace and access to employment opportunities. Incorporating gender perspectives in policy making, or gender mainstreaming,[68] is not a new concept and can be seen in other areas of tech policy such as cybersecurity.[69] Through analysis, identifying gender specific needs, engaging diverse stakeholders, and integrating gender considerations in every stage of policy development, policy makers can influence the development and amendments of laws and regulations to ensure a fairer world for women. This approach is evident in amendments to property rights, marriage, and workplace discrimination.

While gender mainstreaming is not a new concept in policy making, more attention on tech policy is needed in upcoming digital advertising reforms which will also feed into the development of policy and regulation around AI.

It’s no coincidence the biggest players in digital advertising are also the ones forging ahead with AI, powered by the data they are amassing.

An inspiration throughout this project has been the work of Catherine D’Ignazio and Lauren F.Klein. Their book, *Data Feminism*, provides us with a roadmap to thinking differently about data and design. They write that data feminism is *“a way of thinking about data, both their uses and their limits, that is informed by direct experience, by a commitment to action, and by intersectional feminist thought.”* As governments grapple with how to regulate areas of AI, the question of who collects and controls data and its uses is a global priority. The principles of data feminism are: Examine power; challenge power; elevate emotion and embodiment; rethink binaries; embrace pluralism; consider context and make labour visible. If embraced, this way of thinking and the principles would complement gender mainstreaming in tech policy.

To embed this thinking, this chapter analyses several of those efforts from a gender perspective with a focus on women’s health and FemTech.

Data Protection

Sitting here in the EU and UK, surely women are covered by data protection and have nothing to worry about? After all, most relevant to this study, data concerning health, sex life, sexual orientation, racial or ethnic origin, and religious beliefs are considered “special category data” under Article 9 of the GDPR.[70] This type of personal data, along with trade union membership, political opinions, genetic data, and biometric data for identification are singled out as sensitive and merit special protection. The ICO explains why:

“This is because use of this data could create significant risks to the individual’s fundamental rights and freedoms. For example, the various categories are closely linked with: freedom of thought, conscience and religion; freedom of expression; freedom of assembly and association; the right to bodily integrity; the right to respect for private and family life; or freedom from discrimination.

The presumption is that this type of data needs to be treated with greater care because collecting and using it is more likely to interfere with these fundamental rights or open someone up to discrimination.”[71]

"Data concerning health" is defined in the GDPR as *"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."* It's broad, because a lot can be inferred or revealed about someone's health from a wide range of data.

There are additional conditions on processing special category data, beyond the standard conditions, that give extra protection. For example, special category data cannot be processed without explicit consent, whereby the user agrees to the specific sharing of their special category data and is told how the data will be used and by whom. As there are no special protections explicitly for women or reproductive rights as a protected category, this is absolutely key from a gender perspective. However, it is often unclear what it means in practice and how explicit consent is presented to users as a choice.

Many FemTech applications and devices collect sensitive and personal health data, including menstrual cycle information, fertility data, sexual activity details, and more.

Users may not always be fully aware of how their data is collected, stored, and shared.

The GDPR was passed in 2016 and came into force on 25th May 2018. The Data Protection Act 2018 is the UK's implementation of the EU GDPR and was retained after the UK left the EU. The GDPR triggered civil society action[72] to test companies' compliance with the law and there was a flurry of enforcement, especially where "special category data" was concerned. In the UK, the ICO took aim at the data broker industry early on. A 2018 ongoing investigation into direct marketing in the data broking industry found *"...systemic data protection failings across the data broking sector. The Commissioner is concerned that non-compliance with key principles of data protection law appears to be widespread within an industry that depends on personal data."*[73]

In a 2019 profile of data brokers in the Financial Times, the data protection commissioner at the time, Elizabeth Denham, politely pointed to a *"dynamic tension"* between the way data broker businesses are conducted and principles of the GDPR.[74] Subsequent investigations and regulatory enforcement pointed to just how widespread the problem was. Before 2018, many companies were aware of the value of their first-party data to advertisers and dabbled in data brokering. Parenting advice site Emma's Diary, for example, illegally collected data and sold it to the Labour Party for help in profiling new mums, activity that resulted in the site being fined £140,000 in 2018.[75]

In April 2019, another parenting club, Bounty, was fined £400,000 for illegally sharing the personal information of 14 million mums and babies with 39 companies including the credit reference agency Equifax and the data broker Acxiom as part of its services as a data broker.[76] Alongside its decision, the ICO said, *"The number of personal records and people affected in this case is unprecedented in the history of the ICO's investigations into the data broking industry and organisations linked to this… Such careless data sharing is likely to have caused distress to many people, since they did not know that their personal information was being shared multiple times with so many organisations, including information about their pregnancy status and their children."*[77]

As the GDPR settled in, there were fewer incidents of companies selling databases packed with personal data. However, data sharing has in some areas evolved to be craftier and more complex, making non-compliance harder to catch and the harms more difficult to uncover.

Regulation of medical devices

Academics highlight that closer attention needs to be paid to the regulation of FemTech. In *Monitoring Female Fertility Through 'FemTech': The Need for a Whole-System Approach to Regulation*, Catriona Macmillan argues that *"regulation, as it is currently constructed, is insufficiently sensitive to feminist perspectives regarding what these technologies mean for women"*[78] — from data protection to reliability of product claims such as contraception to potential for surveillance.

> As a growing industry, there is increasing scrutiny of the regulation of FemTech, not only from a data protection perspective but also the complicated landscape of medical devices.

The latest guidance from the UK's Medicines and Healthcare Products Regulatory Agency (MHRA) gives examples of software and apps *"which meet the definition of a medical device"* and it outlines *"requirements for UKCA [UK Conformity Assessment] marking of medical devices"*. The guidance includes a category on *"control of contraception"*, namely *"devices that claim to be directly able to make pregnancies more likely or to be able to prevent pregnancy."*[79]

Regulators also need to be wise to companies trying to slip under the radar of the medical regulators. In their 2022 study *Caring for Intimate Data in Fertility Technologies*, which analyses fertility apps within the GDPR, Maryam Mehrnezhad and Teresa Almeida found that most of the 30 fertility apps analysed *"are classified as 'Health & Fitness', a few as 'Medical', and one as 'Communication'."* They added, *"miscategorising an unsecure app which contains medical records (such as user's medical conditions and/or medicines) as Health & Fitness would enable the developers to avoid the potential consequences, for example, of remaining in the app market without drawing significant attention to it."*[80]

Legislative Leaps

The United Kingdom (UK)

The Department for Culture, Media, and Sport (DCMS) in the UK has proposed new digital advertising legislation in an ongoing consultation *"to tackle the evident lack of transparency and accountability across the whole supply chain."*[81] The new legislation intends to prioritise "illegal" advertising, especially to under 18s.[82] This is certainly a start, but it is low-hanging fruit and potentially already covered by the Online Safety Bill.

A supporting analysis of digital advertising harms commissioned by DCMS puts illegal, malicious, and fraudulent adverts as the top categories in a taxonomy of harms, with "discriminatory targeting" and "targeting vulnerable people" at the bottom.[83] On one hand, the reasoning behind selecting these top categories is understandable given that these kinds of adverts are visible to many people. It is harder to see discriminatory ads or those targeting the vulnerable because they are tailored to individuals and are less visible as a result.

However, discriminatory targeting and targeting vulnerable audiences are the categories of harm that are acutely relevant for women. Women are not helpless, powerless, or the eternal victim. But there are situations where women are vulnerable, perhaps temporarily, perhaps more long term. This needs to be addressed.

> Women are not helpless, powerless, or the eternal victim.
>
> But there are situations where women are vulnerable, perhaps temporarily, perhaps more long term.
>
> This needs to be addressed.

Data extracted from women without their knowledge or consent can be exploited in endless ways at points of vulnerability. Likely scenarios include targeting slimming aids to women who have just given birth or targeting unnecessary products and treatments at women desperate to conceive or manage menopause symptoms.

Women globally are targeted by unsafe menstrual products[84] and harmful "beauty" procedures like skin bleaching[85] and buttock lifts.[86]

Discrimination in serving job adverts to women is a long-standing problem yet to be solved. Among the findings of a 2021 investigation by Global Witness,[87] which created job adverts on Facebook with no targeting criteria, 96% of the people shown the ad for mechanic jobs were men and 95% of those shown the ad for nursery nurse jobs were women.

Global Witness has asked the UK Equality and Human Rights Commission (EHRC) to investigate whether Facebook's targeting and ad delivery practices breach the Equality Act (2010). EDRi, a network of over 50 European non-governmental organisations (NGOs) has called for European Data Protection Authorities (DPAs) to conduct a full investigation into discrimination in digital advertising in Europe and enact sweeping reforms.[88]

The European Union (EU)

For several years, the EU has wrestled with the problem of making digital advertising less intrusive. In August 2023, the Digital Services Act (DSA)[89] came into force, which signals a potentially huge change to the way the digital advertising industry operates in the EU. As Claire Pershan and Jesse McCrosky at Mozilla Foundation outlined their analysis published by *Tech Policy Press,*[90] the DSA demands transparency of targeting parameters, increased user control over targeting settings, an end to targeting of ads based on the sensitive characteristics (as outlined in Article 9 of the GDPR), and an end to targeting adverts to children. All eyes are on how it will be enforced by the Commission and implemented through codes of conduct by 2025.

> Incorporating a gender perspective in the drafting of DSA codes of conduct would be extremely beneficial, particularly ending targeting based on sensitive characteristics and avoiding advertising to "vulnerable groups" and those in "vulnerable situations."

In addition, the DSA also requires searchable public ad repositories of the largest platforms.[91] An important transparency initiative that will improve over time, this requirement makes ads that were only visible to a target audience a matter of public record.[92] This could go some way towards flagging adverts that are harmful to people in vulnerable situations.

The United States of America (US)

The harms caused by intrusive digital advertising, particularly the activities of data brokers and online platforms has a high profile in the US. Most tech companies, including the largest data brokers are established in the US and there is currently no federal privacy or data protection law, although this is in the works.[93]

> While the EU and UK lean heavily on data protection, the US approaches the issue from a consumer rights angle.

At an event at the White House in August 2023, The Consumer Financial Protection Bureau (CFPB) announced that it will issue proposed rules ensuring that certain data brokers would be prohibited from selling data for purposes other than those authorised under the Fair Credit Reporting Act (FCRA).[94]

The House Judiciary Committee is also advancing the Fourth Amendment is Not for Sale Act[95] to prevent data brokers selling consumer data to law enforcement and federal agencies, which would effectively enable them to bypass obtaining a warrant. The name of the act reflects the Fourth Amendment of the Constitution, which protects against warrantless searches.

California law requires a data broker to register on the Attorney General website or face a $10,000 fine.[96] As a result, there is a public register of over 500 data brokers including contact information and information on how to opt out under the California Consumer Privacy Act (CCPA).[97] This is an innovative way to bring transparency to the industry and increase attention on companies that are not consumer facing.

Arguably the biggest jolt to moving privacy protection forward in the US came from an issue directly impacting women's reproductive rights. In June 2022, the US Supreme Court overturned Roe vs. Wade in the case of Dobbs vs. Jackson Women's Health Organisation, striking down the constitutional right to abortion established nearly 50 years earlier. Individual states began implementing their own laws outlawing abortion and it sent lawmakers working on digital rights into a spin.[98]

Investigations into the dangers of digital surveillance and how women's data could be used to criminalise them for seeking abortions came thick and fast. Gizmodo published the results of an investigation into the types of information concerning millions of women that data brokers regularly transact. In one case, a data broker offered a catalogue of people using the same kind of birth control that many states are trying to outlaw.[99] Acxiom, a major data broker, was forced by shareholders to publicly state it would not collect location data from abortion clinics.[100] Meta was criticised for handing over Facebook Messenger chats that resulted in the prosecution and ultimate incarceration of a mother for helping her teenage daughter obtain abortion pills in Nebraska.[101]

The overturning of Roe vs. Wade sent ripples around the world as to the real-life impacts of data sharing for women. FemTech companies were about to step into the storm.

Chapter Seven: Enter FemTech

"Health apps are in the midst of a privacy and security reckoning."

- Flo Privacy and Security Advisory Board member.[102]

The growth of the FemTech industry has come with intense scrutiny. Period and fertility trackers were on the radar of many civil society organisations prior to the overturning of Roe vs. Wade. Investigations by Privacy International, The Norwegian Consumer Council, Consumer Reports, Mozilla's Privacy Not Included, and ORCHA[103] highlighted concerns around data collection and sharing of sensitive data. A few months after the overturning of Roe vs. Wade, one US study found women's health apps to be the least trusted.[104] What can be done?

To move towards positive changes, this project engaged with the FemTech industry in the UK, the EU, and the US. An online survey ran throughout Summer 2023, which solicited 48 responses from C-suite executives, investors, and marketing professionals in the FemTech industry. Three roundtable discussions and interviews featuring a total of 13 FemTech founders, investors and marketing/advertising experts took place remotely in September 2023 under Chatham House rules.

The discussion focused on reforms needed in the digital advertising industry, demonstrating far reaching impacts for consumer-facing businesses and their obligations and desire to protect their customer privacy. The following themes reflect common issues raised in the discussions and weave in results from the industry survey — they do not necessarily reflect the views of all participants.

Theme: Building Trust

Each roundtable discussion began with a key finding from the consumer survey and a question:

44% of 1,000 women surveyed said they had deleted an app because of privacy concerns. When asked to specify which app, 20% specified it was a period or fertility tracking app. Why do you think this is and what can the industry do to build trust?

On the whole, roundtable participants were not completely surprised by these findings, believing that they reflect mistrust in health services generally and that women feel let down by health services.

> When asked how to build trust, participants advocated for radical alternatives and innovative models rather than tweaking the current system.

> Participants overwhelmingly felt that their customers care about privacy and that 'big tech' has dehumanised consumers.

Participants raised concerns about targeted adverts that have an inadvertently negative impact on consumers' mental health, given that FemTech products are trying to achieve the opposite. Participants put great value on listening to their users and building relationships with them, which they believe reveal more insights than any data point could. Health and wellness needs must be at the centre of the business, rather than exploited for commercial purposes without consent.

Theme: The Business Model

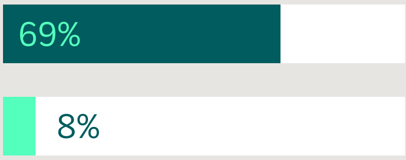
Participants stressed that they do not sell user data and would cut off connected revenue streams to build trust and protect user privacy.

> One question that remains open is the degree of pressure from investors to monetise data as part of a business model by selling it to third parties.

It was suggested that most male investors assume that women lack purchasing power and selling data therefore must be the business model rather than, for example, a subscription-based model. A strong perspective from the discussion centred on how to diversify revenue away from monetising data and towards connecting value to products by starting to build models and demonstrating that they are profitable prospects.

Theme: Engaging with Digital Advertising

Findings from the FemTech industry survey were then discussed by the roundtable participants.



69% undertook some form of digital advertising.
Only 8% of respondents felt that the digital advertising industry operates in a clear and transparent way.

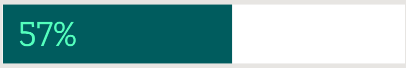
Respondents felt that once a business is up and running, advertising on social media is key to grow the business and reach women who may be struggling with symptoms or conditions that their products can help with. However, FemTech companies experience obstacles to advertising on social media, with ads censored or rejected for featuring words like “vagina.” This causes confusion, and ultimately reinforces stigma and taboos around the discussion of women’s bodies.[105]

Roundtable participants felt that the opaqueness of the online advertising industry was by design, and it is in their interest to present an all-powerful “black box.” The feeling was that FemTech companies don’t have to accept this status quo.

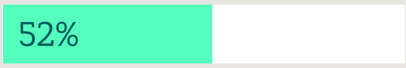
Over half of survey respondents were not confident they had a clear understanding about which third parties have access to customer data.

> On one hand, the industry is complex and opaque. On the other, failing to have a full picture of which third parties have access to customer data is unacceptable.

This will ultimately damage a company's reputation and undermine trust if they are viewed as being reckless with their customers' data. A lack of visibility into the data value chain also puts the company at risk of regulatory non-compliance.



57% said their business does not rely on monetising customer data.



However, 52% of industry respondents said they had installed some kind of analytics or retargeting tools such as the Meta pixel.

> Selling customer's personal data is a no-no recognised by many in the industry. However, it is not enough for companies to say they don't sell data and sit back.

When it comes to digital advertising tools, companies are cornered into using "industry standard" methods such as installing pixels and using SDKs that extract large amounts of personal data. The company might not be monetising data, but some actor somewhere in the ecosystem likely is.

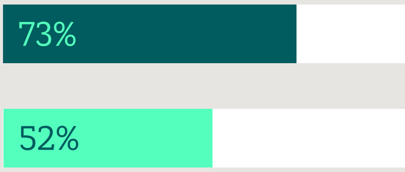
Tracking capabilities are embedded deeply into many popular analytics tools and developer toolkits used by companies to build their products, such as the "Meta pixel," a piece of code a developer puts on their own website to track users' activity on that website and help with targeting or retargeting users with advertising on Facebook.[106] A 2023 investigation by *The Guardian* in the UK revealed the NHS, the Metropolitan Police and several mental health charities were sharing sensitive data in this way.[107]

This has not yet led to any regulatory action under data protection law in the UK, but it has in the US under consumer protection law. The FTC has advocated around the hidden impact of pixel tracing.[108] In 2019, the FTC settled with Flo Health regarding the complaint that it shared sensitive health data from millions of users of its Flo Period & Ovulation Tracker app with marketing and analytics firms, including Facebook and Google.[109]

The FTC found BetterHelp, an online counselling app whose users are reportedly mostly young and female,[110] continually broke its privacy promises bysharing data extensively with Facebook, monetising consumers' sensitive health information to target them and others with advertisements.

Part of the FTC complaint against Premom, an ovulation tracker, detailed how the company requested access to a customer's location to pair a bluetooth thermometer, and then shared that precise location data with two analytics firms based in China, which could then sell that information to others. In an extraordinary statement, the FTC said Premom's actions were likely to cause *"stigma, embarrassment, or emotional distress, and may also affect their ability to obtain or retain employment, housing, health insurance, disability insurance, or other services."*[111] This impact points squarely to discrimination and the FTC found this case to be so serious it barred Premom from sharing health data for advertising.[112]

Theme: Struggling with Privacy Policies



73% felt there is not enough information from regulators to help the business comply with its data protection obligations.

52% felt that privacy policies are not the best way to inform customers about what happens to their data.

While it was felt that GDPR has set the ground rules for how to shape a business, participants struggle to communicate data protection principles in a way that connects with the user. Many also require a better method of explaining to users what their data is used for.

The unpopularity of privacy policies and Terms of Service (ToS) are well documented. Nobody likes them, nobody reads them, and they have a bad name for being lengthy, complex, and dishonest.[113] In *Caring for Intimate Data in Fertility Technologies*, Mehrnezhad and Almeida home in on how terms explain sharing data with third parties:

"For the most part, these are connections established via fine-print privacy policies and terms-of-service agreements and while technically permissible under such terms, violate user expectations and contextual norms. Such data-sharing practices abound and, while the 'data subject' might be asked to give their consent prior to the gathering and processing of their data, it is less clear how well that individual consent is informed consent or what exactly will happen to the data gathered afterwards."[114]

ToS and privacy policies are two distinct legal documents. The ToS defines the legal relationship between the service and the user, outlining the rules of using the service. Users typically must accept or agree to the ToS before using a service. A privacy policy relates to data protection and privacy, and provides information about data collection, sharing and storage, and the privacy rights of the user.

As Mozilla Fellow Bogdana Rakova writes, *"I agree to the terms of services is perhaps the most falsely given form of consent."* In her research exploring alternatives to platform's terms of service, she highlights the lack of bargaining power and the need for consumers to be given an actual choice.

Bogdana has developed the "Terms-we-Serve-with" framework as an alternative.[115] A central dimension of the framework is that of co-constitution, that terms are co-designed with the community to build in transparency and awareness from the outset. This is a bold reimagining of how a ToS could be manifested in the future, which aligns with both gender mainstreaming in policy making and data feminism theory. The approach serves as a challenge to the power imbalance that traditionally controls, restricts, and ignores female autonomy and lived experience online as well as offline.

To be fit for purpose, FemTech privacy policies should look to address gender-influenced issues including data minimisation, how special category data is handled, and how users can opt out and delete their data simply and quickly.

Theme: The Hunt for Alternative Digital Advertising Models

49% have explored alternative advertising methods.

A central theme through this project has been the focus on alternatives to the current digital advertising models. As outlined in earlier chapters there is a cat-and-mouse game between those trying to restrict online tracking and those trying to find workarounds.

There is a clear desire for advertising models that rely less on personal data and tracking people across services, however these are still a work in progress.

This moment represents an opportunity for policymakers and regulators to support innovation in alternative advertising methods.

We explore some of the current debates below.

1. Privacy preserving attribution methods.
One of the puzzles for industry is how to find out how ad campaigns are performing in a privacy respecting way. Known as attribution, advertisers want accurate reporting about how their ad campaigns are performing and which ads resulted in customer purchases. Today, this means engaging in tracking and identifying users. However, the effectiveness of attribution is contested, even by those in the industry. This further supports the contention that over-reliance on user tracking and the resulting harmful impacts are all for little gain.[116]

In response to investigations around pixels and SDKs, some roundtable participants report that they are working on in-house analytics solutions to avoid outsourcing to other companies and potentially losing control of their data. There are efforts in other forums to advance this issue; For example, Mozilla and Meta have jointly proposed Interoperable Private Attribution (IPA) for measuring attribution without tracking.[117]

> Some roundtable participants identified that user anonymity is so important to their FemTech business they accept they cannot conduct attribution under the current system because of the reliance on digital identifiers.

2. The problem with Identifiers
As mentioned earlier, tracking users involves tying each individual to a unique ID to link profiles across different services, devices, and platforms. As platforms make moves to phase out third party trackers, the humble email has come under the spotlight.

> Email addresses are the new cookies.

Many services require an email address to register, which can be used to cross-reference against other sources and build a profile. Emails are requested when making a purchase or signing up to a subscription, by any company that needs to communicate with you. It is possible for services that don’t need to communicate with you not to ask for this, like a Virtual Private Network (VPN), however that is not the model of the FemTech industry. Every time an email address (or telephone number) is entered to access a service, it serves as a unique identifier that can link activity across the web. The Electronic Frontier Foundation (EFF) has warned of the tracking potential through email addresses.[118]

Your email address is “hot commodity”, as Mozilla explains:

“Most people have only one or two email addresses, yet they have dozens, if not hundreds, of online accounts connected to them. Your email address is a unique identifier — after all, you’re the only one with it. And that means a good deal of data is associated with it, making your email address a desirable target.”[119]

Email identifier masking for users exists – like Firefox Relay or Apple Hide My Email – however this is another responsibility pushed onto the user. It is very difficult to solve on the developer side.

Collecting customer emails as first-party data will be essential in a subscription-based business model. Roundtable participants spoke of the challenge of collecting first-party data while also protecting it to the highest standard. Some discussed the turmoil post Roe vs. Wade, looking inwards at how data was secured technically and how they would respond if approached by law enforcement in the US to hand over a woman’s data. The debate also covered the importance of encryption, where the data is stored, protecting against unauthorised access and anonymisation.

However, some participants understand that the most reliable form of anonymisation is not to collect data in the first place. Post Roe vs. Wade and their own brush with the FTC, one of the largest ovulation and period trackers, Flo, introduced an “Anonymous Mode” allowing the service to be accessed *“without any personally identifiable information, such as a name, email address, and technical identifier being associated with the account.”* Flo open-sourced the Anonymous Mode and published the code on Github.[120]

Chapter Eight: A Way Forward: Summary

As we experience a global backlash against women's rights and hard-won legislative progress is being rolled back, the rise of the FemTech industry is simultaneously empowering women to take control of their own health and plugging gaps in access to and research on women's healthcare. But as women turn to technology for support during vulnerable life moments, they are open to exploitation as a result of the complex and opaque digital advertising industry that underpins the internet.

The most lucrative internet business model is collecting personal data that is used to target people with online ads. It is no secret that there are major concerns for regulators, government policymakers, advertisers, and the public about the intrusive nature of the online advertising industry. As we move into the age of AI, we cannot repeat the mistake of the 1990s that left tech companies essentially unregulated in the name of innovation.

This study advocates for incorporating a gender perspective into ongoing digital advertising reform in the UK and EU, with the goal of protecting women's privacy and spurring a cultural shift to reframe our relationship with tech companies. It will require ongoing legislative and regulatory reform and practical actions from industry to develop alternative advertising models to reduce harm.

Outline of Harms

- Maintaining control over personal and intimate information is paramount for women's safety, particularly in situations where they are temporarily vulnerable.
- Women experience more moments of specific or temporary vulnerability such as seeking fertility treatment, giving birth, managing the menopause. We need to ensure that these moments of vulnerability do not lead to exploitation.
- Many FemTech applications and devices collect sensitive and personal health data, including menstrual cycle information, fertility data, sexual activity details, and more. Users may not always be fully aware of how their data is collected, stored and shared, which can put women at risk both online and offline.
- Excessive data collection potentially puts women in a perpetual state of vulnerable situations as data extracted from women without their knowledge or consent can be exploited in endless ways.
- Likely scenarios include targeting slimming aids to women who have just given birth or targeting unnecessary products and treatments at women desperate to conceive or manage menopause symptoms. Women globally are targeted by unsafe menstrual products and harmful "beauty" processes like skin bleaching and buttock lifts.
- The impact of being targeted with adverts for unwanted pregnancy products, for example after suffering a miscarriage, can have a negative impact on mental health. On an individual level, this type of targeting risks causing unnecessary feelings of shame and grief. On a societal level it perpetuates gender norms and reinforces stigma and taboos around discussions of women's bodies already deep rooted in society.
- Women are at the mercy of who is collecting and interpreting their data and making assumptions about their lives. This has real-life impacts when these assumptions are based on reproductive issues and data such as location, online searches, online shopping habits and suspected missed periods that can be weaponised and used to prosecute women for seeking an abortion.

Barriers to change

- Taboos around discussing women’s bodies, poor funding, limited research for women’s health, and a lack of investment in female-led businesses.
- Harms such as discrimination and targeting those in vulnerable situations are less visible and build over time and therefore are often lower on the list of priorities for policymakers to tackle. However, these are the categories of harm that are acutely relevant for women.
- Women do not experience the same threats or vulnerabilities at the same time, known as “differential vulnerabilities” — there is no “one size fits all” solution.
- The digital advertising industry is opaque and complex to navigate and understand, both from a user and an advertiser perspective.
- The expectation and responsibility is weighted against the individual to manage their own privacy online, which is impossible to do comprehensively.
- As there are no special protections explicitly for women as a protected category, the rules around special category data are absolutely key from a gender perspective. However it is often unclear what protections on special category data means in practice and how explicit consent is presented to users as a choice.
- As some technology is phased out, other tracking methods surface, leading to a cat-and-mouse game between those actors trying to improve online protections and those trying to work around them or find loopholes.
- A lack of understanding around “industry standard” tools such as installing pixels and using software development kits (SDKs) that extract large amounts of personal data.
- There is a clear desire for advertising models that rely less on personal data and tracking people across services, however these are still a work in progress.

Chapter Nine: Recommendations for Action

For Policymakers: Priorities for Reform

Analyse

Conduct gender-focused research on the harms of digital advertising. There is clearly a need to listen more closely to women's concerns around data collection and sharing as it relates to their safety and wellbeing. While studies on public awareness of data collection and use exist, there are few with a gender focus. Analysing the problems from a gender perspective reveals that the gratuitous data collection that forms the root and branch of online advertising has a unique impact on women and their privacy, particularly around reproductive rights such as menstruation, sex, pregnancy, IVF, birth, miscarriage, abortion and menopause.

Recognise

The importance of protecting women's data as a safety issue. Consider a ban on the sharing of sensitive personal data altogether for advertising purposes, including analytics and attribution as the FTC did in the case against Premom in the US. This could be particularly impactful in EU markets with restrictive laws around reproductive rights.

Data protection cannot be enjoyed when so much of the industry is hidden and poor compliance can be hard to catch. Too much personal data is collected in an opaque way. Policymakers could consider ways to bring AdTech companies and data brokers, which are not consumer facing, out of the shadows by implementing a public register of data brokers with penalties for not registering.

Data protection should not take all the regulatory burden. The UK and EU rely heavily on data protection to curb the negative impacts of digital advertising. The US has taken a different regulatory approach in absence of federal data protection laws by leaning on consumer protection frameworks such as the Federal Trade Commission Act and the Health Breach Notification Rule which has enabled enforcement in some of the more complex areas of AdTech such as the role of pixels and SDKs. Policymakers could consider replicating this approach to widen regulatory options.

The importance of ad libraries for transparency. Requiring searchable, public ad libraries as outlined in the EU's Digital Services Act make adverts that were only visible to a target audience a matter of public record and assists in flagging adverts that are harmful to people in vulnerable situations.

The development of new harmful tracking techniques. As tracking techniques such as third-party cookies are phased out, others are developed such as browser fingerprinting and increased reliance on email as a unique identifier.

Invest in

Research on discriminatory targeting and targeting the vulnerable with a gender perspective.

Female founders and female-led businesses as part of implementing strategies for women's health, alternative digital advertising models and the future of AI.

Innovation to grow alternative business models. To revolutionise the digital advertising industry, we need to rely less on the collection of personal data by stemming the flow of personal data and reducing the value. This would benefit from government support and investment to develop and grow new business models that do not rely on monetising data.

Testing alternative digital advertising models. Regulation bites, but without investment in technical alternatives and innovation, we enter a cycle of regulatory fines. There is a demand for alternatives, but investment is needed. As part of its commitment to reforming online advertising, governments could fund a series of companies to test ideas for alternatives.

For Regulators: Priorities for Support and Enforcement

Bring data brokers out of the shadows. Data brokers for too long have been able to slip through the cracks of regulation and hide behind "invisible processing." Support the recommendation for a public register of data brokers.

Launch an investigation into pixels and SDKS. Home in on the extractive nature of SDKs and pixels from a data protection perspective.

Include deletion orders in enforcement notices where data has been found to be illegally collected.

Explore alternative ways to communicate how to present information in a privacy policy. Frameworks such as "Terms-we-Serve-with" could provide a starting point for a bold reimagining of this area, such as those co-designed with the user community to embed transparency and awareness from the outset.

For FemTech Founders: Priorities for Action

Engagement with the FemTech industry throughout this project has been very positive and has demonstrated some clear actions companies can implement now and a move towards best practice. Data is hugely important for advancing women's healthcare, but protecting this data from exploitation is imperative. These recommendations are presented as a starting point for discussion on due diligence and best practice.

Data Audits, Safety and Communication: It is Not Enough to Say "We Don't Sell Your Data."

Minimise data collected. A key safety feature is taking steps to reduce data collection in the first place. Do you really need all the data e.g., location data?

Storage location. Do you know where data is stored? Can you change the location of storage if there is a threat to women's safety e.g., a change in abortion laws? Has the company discussed how it would respond if law enforcement requested access to customer data? Store data locally on the device rather than remotely on a server.

Third parties. It is unacceptable not to know which third parties have your customer data.

- Ensure you know which third parties have data and these parties are clearly published in your privacy policy.
- No more generic use of the label "third parties." Directly name all companies in your privacy policy that have access to or analyse customer data.
- Remove tracking tools and pixels, such as the Meta pixel, from websites.

Give customers clear options for control, such as clear ways to opt out, clear paths to delete data including emergency deleting of apps and accounts if under threat.

Keep exploring alternatives, share findings with the FemTech industry community and other allies.

- When engaging with digital advertising, only advertise in the broadest of categories and share little to no data with platforms.
- Think about your sign-up model and ways to build growth without relying on an email identifier.

Engage with government reforms and regulators

- Seek support from regulators. For example, at the time of writing the ICO offers a regulatory sandbox to test and embed privacy by design into products and services.
- Engage with legislative reforms in the EU and UK. The European Commission will consult on codes of conduct around digital advertising and the UK government plans to further consult on the adoption of digital advertising legislation. Ensure a gender perspective and the issues faced by the FemTech industry are incorporated.

Endnotes

[1] BBC (January 28th 2021) *"Coronavirus: Government withdraws 'sexist' Stay Home advert"* BBC News [online].

[2] Bergsten, S., Lee, P.S.A. (March 18th 2023). *"The Global Backlash Against Women's Rights: A Stark Reminder on International Women's Day."* Human Rights Watch.

[3] European Union, UN Women, Imkaan. *"The Value of Intersectionality in Understanding Violence Against Women and Girls (VAWG),"* July 2019.

[4] Winchester, N. (2021). *"Women's Health Outcomes: Is There a Gender Gap?"* In Focus, House of Lords Library.

[5] Statista (2023) *"Digital advertising expenditure in the United Kingdom (UK) from 2008 to 2022."*

[6] A 2022 study from Nord VPN showed that on average UK websites contain 18.6 trackers.

[7] Recognising the work of Privacy International, The Norwegian Consumer Council, Check My Ads, NOYB, Wolfie Christl, Dr. Johnny Ryan and Mozilla Fellows present and alumni Harriet Kingaby, Frederike Kaltheuner, Karolina Iwańska, Chenai Chair, Bogdana Rakova, Brandi Geurkink and Julia Keseru.

[8] For more on feminist research methodology, see Wambui, J. (2013). *"An Introduction to Feminist Research,"* University of Nairobi and Chenai Chair (2020) *"A Feminist Approach to Right To Privacy and Data Protection."*

[9] NASA Johnson Space Center Oral History Project. (2002). Oral History Transcript: *Sally K. Ride, Interviewed by Rebecca Wright.* San Diego, CA – 22 October 2002.

[10] NASA History (2018) *"Sally Ride – First American Woman in Space"* NASA [Online].

[11] Winchester, N. (2021).

[12] British Heart Foundation (2019) *"Heart attack gender gap is costing women's lives"* BHF [online].

[13] BBC (May 29th 2018) *"Everybody was telling me there was nothing wrong"* BBC Future [online].

[14] MBRRACE-UK (2021) *"Saving Lives, Improving Mother's Care. Lay Summary 2021"* p2 and Mundasad, S (November 11th 2021) *"Black women four times more likely to die in childbirth"* BBC News [online].

[15] NHS England, *LGBT health* BBC [online].

[16] Endometriosis UK *"Endometriosis Facts and Figures"* [online].

[17] Royal College of Obstetricians and Gynaecologists (RCOG) (2022) *"Left for too long: Understanding the scale and impact of gynaecology waiting lists"* [online].

[18] Bishen, S., Ali, K., & World Economic Forum. (2023). *"Women's Health: Rethinking the Cost as an Investment for Societal Gain."*

[19] Jillian Levovitz, MBA, Elizabeth Gordon, Carley Prentice, MPH, Brittany Barreto, PhD, Yedidiah Teitelbaum, (2023) *"FemTech Landscape 2022"* FemHealth Insights.

[20] Statisia (2022) *"FemTech market size worldwide from 2021 to 2030."*

[21] Smith, K (2023) *"Women's health research lacks funding- these charts show how"* Nature.

[22] British Business Bank (2019) *"UK VC and Female Founders Report"*.

[23] Department of Health and Social Care (2022) *Women's Health Strategy for England,* UK Government.

[24] Keats Citron (2023) pp14-15.

[25] BBC 5 Live (May 9th 2023) *Naga Munchetty* [online].

[26] Ibid.

[27] Vernon, H. (2023). *Etihad Airways Worker Used Airline Data to WhatsApp Me, Says British Woman*. The Guardian.

[28] Renee Shelby, Shalaleh Rismani, Kathryn Henne, AJung Moon, Negar Rostamzadeh, Paul Nicholas, N'Mah Yilla-Akbari, Jess Gallegos, Andrew Smart, Emilio Garcia, and Gurleen Virk. 2023. *"Sociotechnical Harms of Algorithmic Systems: Scoping a Taxonomy for Harm Reduction."* In AAAI/ACM Conference on AI, Ethics, and Society (AIES '23), August 8–10, 2023, Montréal, QC, Canada. ACM, New York, NY, USA, 19 pages.

[29] Zuboff, S. (2019) Chapter 3: The Discovery of Behavioural Surplus, pp 63-97.

[30] See Information Commissioner's Office (UK), *"What is microtargeting?"* [online].

[31] See Rosenberg, M., Confessore, N., & Cadwalladr, C. (2018, March 17). *"How Trump Consultants Exploited the Facebook Data of Millions."* The New York Times.

[32] Federal Trade Commission (FTC) July 24th 2019, *"FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook".*

[33] European Commission, Directorate-General for Communications Networks, Content and Technology, Armitage, C., Botton, N., Dejeu-Castang, L. et al., *Study on the impact of recent developments in digital advertising on privacy, publishers and advertisers – Final report*, Publications Office of the European Union, 2023 p138.

[34] See Wood, M (September 3rd 2019) *"Today's Firefox Blocks Third-Party Tracking Cookies and Cryptomining by Default"* Mozilla blog and Statt, N (March 4th 2019) *"Apple updates Safari's anti-tracking tech with full third-party cookie blocking,"* The Verge. Google intends to phase out third party cookies in Chrome by 2024, Mihajlija, M (May 17th 2013) *"Prepare for phasing out third-party cookies"* Chrome for developers blog.

[35] Fox-Brewster, T. (October 3rd 2014) *"Check the Permissions: Android Flashlight Apps Criticised Over Privacy."* The Guardian.

[36] See ICO (October 2020) *"Investigation into data protection compliance in the direct marketing data broking sector"* p21.

[37] The Competition and Markets Authority (CMA) (2020) *Online Platforms and Digital Advertising Market* Study. *See Appendix G: The role of tracking in digital advertising* p1

[38] Keegan, J., & Eastwood, J. (June 8th 2023). *"From 'Heavy Purchasers' of Pregnancy Tests to the Depression-Prone: We Found 650,000 Ways Advertisers Label You."* The Markup.

[39] Privacy International (2019) *"Why am I really seeing that ad? The answer might be Real Time Bidding (RTB)".*

[40] Achara, J. P., Acs, G., Castelluccia, C. (2015). *"On the Unicity of Smartphone Applications."* ACM CCS Workshop on Privacy in Electronic Society (WPES) 2015. See also: de Montjoye, YA., Hidalgo, C., Verleysen, M. *et al. "Unique in the Crowd: The privacy bounds of human mobility". Sci Rep* 3, 1376 (2013).

[41] Cox, J. (May 17th 2022). *"Data Marketplace Selling Info About Who Uses Period Tracking Apps."* Motherboard.

[42] Cristl, W. (2017). *"Corporate Surveillance in Everyday Life: How Companies Collect, Combine, Analyze, Trade, and Use Personal Data on Billions."* Cracked Labs p5

[43] ICO (2020)

[44] European Commission (April 28th 2023) *"Cookie Pledge. A reflection on how to better empower consumers to make effective choices regarding tracking-based advertising models."* [online].

[45] See Mozilla blog *"Firefox blocks fingerprinting."*

[46] Benjamin, R (2019) pp 74-75.

[47] Garamvolgyi, F. (June 28th 2022). *"Why US Women Are Deleting Their Period Tracking Apps."* The Guardian.

[48] Brodkin, J. (May 25th 2022). "Google Urged to Stop Collecting Phone Location Data Before Roe v. Wade Reversal." Ars Technica.

[49] See, Reuters (May 3rd 2022) *"The World's Toughest Abortion Laws."*

[50] Channel 4 News Investigations Team (September 28th 2020) *"Revealed: Trump campaign strategy to deter millions of black Americans from voting in 2016"*, UK.

[51] Graham- Harrison, E (February 28th 2021) *"Leave.EU donor Arron Banks loses data breach appeal".* The Guardian.

[52] Bright, S (August 3rd 2017) *"After Trump,"big data" firm Cambridge Analytica is now working in Kenya",* BBC News online.

[53] Cox, J (September 16th 2020) *"How the U.S. Military Buys Location Data from Ordinary Apps"*, Motherboard.

[54] Benjakob, O (September 23rd 2023) *"Revealed: Israeli Cyber Firms Have Developed an 'Insane' New Spyware Tool. No Defense Exists"*, Haaretz.

[55] Harwell, D (April 10th 2019) *"Is your pregnancy app sharing your intimate data with your boss?"*, The Washington Post.

[56] Glenza, J (May 30th 2019) *"Revealed: women's fertility app is funded by anti-abortion campaigners",* The Guardian.

[57] Topping, A (October 2nd 2023) "*Women's rights held hostage at UN, say former leaders"*, The Guardian.

[58] Mehrnezhad, M and Almeida, T (2021). "*Caring for Intimate Data in Fertility Technologies."* CHI '21: Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems May 2021 Article No.: 409 Pages 1–11

[59] Susanne Barth, Menno D.T. de Jong (2017) *The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behaviour – A systematic literature review,* Telematics and Informatics, Volume 34, Issue 7, 2017, Pages 1038-1058, ISSN 0736-5853.

[60] Mark Rowan, Josh Dehlinger, *"Observed Gender Differences in Privacy Concerns and Behaviours of Mobile Device End Users,"* Procedia Computer Science, Volume 37, 2014, Pages 340-347, ISSN 1877-0509.

[61] ICO (7th September 2023) *"ICO to review period and fertility tracking apps as poll shows more than half of women are concerned over data security,"* Media Centre.

[62] The categories of FemTech outlined in the survey were: Ovulation trackers, period trackers, birth control/contraception, pregnancy tracker, breast feeding, IVF/Fertility, menopause symptom tracker, safe abortion, baby milestones, kegel trainer/pelvic floor exercise, smart vibrator, sex tracking, fitness apps and mental health apps.

[63] Department of Health and Social Care (April 13th 2022) *“Call for evidence”,* Women’s Health Strategy, UK Government.

[64] Hendrix, J (July 14th 2023) *“Rescuing the Future from Silicon Valley,”* Tech Policy Press.

[65] Gestalten (December 2019) *“Cindy Gallop On Ten Years of MakeLoveNotPorn,”* Gestalten UK.

[66] For example, see Emily M. Bender, Timnit Gebru, Angelina McMillan-Major, and Shmargaret Shmitchell. 2021. “*On the Dangers of Stochastic Parrots: Can Language Models Be Too Big?*” In Conference on Fairness, Accountability, and Transparency (FAccT ’21), March 3–10, 2021, Virtual Event, Canada. ACM, NewYork, NY, USA, 14 pages. Abeba Birhane, Vinay Prabhu, Sang Han, Vishnu Naresh Boddeti (2023),” *On Hate Scaling Laws For Data-Swamps*.”

[67] UN Women (December 22nd 2022) *“Announcement: International Women’s Day 2023: “DigitALL: Innovation and technology for gender equality””* and UN Women (March 18th 2023) Press release: “*Press release: UN Commission on the Status of Women reaffirms the role of technology and innovation, and education in the digital age in accelerating gender equality.”*

[68] See, OECD, “*Gender mainstreaming in policymaking.”*

[69] APC (June 30th 2023) *“APC explainer: What is a gender approach to cybersecurity?”*

[70] See Article 9 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[71] See, ICO, *“What is special category data?”*

[72] See Privacy International, *“Timeline of complaints against AdTech.”*

[73] ICO (October 2020) *“Investigation into data protection compliance in the direct marketing data broking sector,”* p38.

[74] Ram, A and Murgia, M (January 8th 2019) *“Data brokers: regulators try to rein in the ‘privacy deathstars,’”* The Financial Times.

[75] BBC Technology (August 9th 2018) *"Emma's Diary fined £140,000 over data sale to Labour,"* BBC News online.

[76] ICO (2018) Data Protection Act 1998. Supervisory powers of the Information Commissioner. Monetary Penalty Notice.

[77] Hern, A (April 12th 2019) *"Parenting club Bounty fined £400,000 for selling users' data."* The Guardian.

[78] Catriona McMillan, *"Monitoring Female Fertility Through 'FemTech': The Need for a Whole-System Approach to Regulation," Medical Law Review*, Volume 30, Issue 3, Summer 2022, Pages 410–433.

[79] UK Medicines and Healthcare products Regulatory Agency (MHRA) *"Guidance: Medical device stand-alone software including apps (including IVDMDs)"* v1.10f, p25.

[80] Mehrnezhad,M and Almeida, T (2021).

[81] UK Department for Culture, Media and Sport (DCMS) (March 9th 2022) *"Online Advertising Programme consultation"*.

[82] UK Department for Culture Media and Sport (DCMS) (July 25th 2023) *"Consultation outcome: Online advertising programme."*

[83] Spark Ninety (July 11th2022) *"Online Advertising Programme Market Insights. Final Report. For the Department of Digital, Culture, Media and Sport,"* pp 16-17.

[84] Nghuhi, W (2023) *"Online Health Scams for Sale. How Google, Facebook, YouTube and Instagram Allow Dangerous Health Products to be Targeted at Kenyan Women. And Make Money From It"*. Fumbua, Kenya.

[85] See, World Health Organisation (WHO) (November 3rd 2019) *"Mercury in skin lightening products*: *Preventing disease through healthy environments".*

[86] Marsh, S (June 2nd 2023) *"Complaints about non-surgical butt lifts 'rising at alarming rate' in UK",* The Guardian.

[87] Global Witness (September 9th 2021) "*How Facebook's ad targeting may be in breach of UK equality and data protection laws*".

[88] EDRi (June 16th 2021) *How online ads discriminate.*

[89] European Union Agency for Criminal Justice Cooperation, *"Digital Services Act – Ensuring a safe and accountable online environment,"* 2022.

[90] McCrosky, J and Pershan, C (August 25th 2023) *"No Perfect Solution to Platform Profiling Under Digital Services Act*", Tech Policy Press.

[91] See Article 30 of the DSA.

[92] Leerssen, P (May 25th 2021) *"Platform ad archives in Article 30 DSA", Institute for Information Law (IViR)*

[93] Taylor Hodges, J (August 24th 2023) *"It's Time to Pass U.S. Federal Privacy Legislation,"* Mozilla blog.

[94] Suleiman, R and Taylor Hodges, J (August 21st 2023) *"Mozilla applauds CFPB for taking on Data Broker Ecosystem,"* Mozilla blog.

[95] Ron Wyden, United States Senator for Oregon (April 21st 2021) *"Wyden, Paul and Bipartisan Members of Congress Introduce The Fourth Amendment Is Not For Sale Act."* Ron Wyden website.

[96] See Civil Code §1798.99.80

[97] Rob Bonta, Attorney General, "*Data Broker Registry,"* State of California Department of Justice

[98] Popli, N and Bergengruen, V (July 1st 2022) *"Lawmakers Scramble to Reform Digital Privacy After Roe Reversal",* Time.

[99] Wodinsky, S and Barr, K (July 30th 2022) *"These Companies Know When You're Pregnant—And They're Not Keeping It Secret,"* Gizmodo.

[100] Sumagaysay, L (March 2nd 2023) *"Large data broker promises not to collect info that could be used in abortion-related prosecutions,"* MarketWatch.

[101] Sherman, C (September 22nd2023) *"US mother sentenced to two years in prison for giving daughter abortion pills,"* The Guardian.

[102] Flo (January 24th 2023) *"Flo Health appoints new executive and launches Privacy & Security Advisory Board to further its commitment to protecting its 50M monthly active users' data."*

[103] See: Privacy International (2019) *"Nobody's Business But Mine"*; The Norwegian Consumer Council (2020) *"Out of Control";* Consumer Reports (2020) "What Your Period Tracker App Knows About You"; Mozilla's Privacy Not Included (2022) *"Reproductive Health"*; ORCHA (2022) *"Data Privacy Matters...Period. Data security of period tracking apps"*.

[104] Epker, E (May 16th 2023) *"Survey Finds Women's Health Apps Are Among The Least Trusted: What To Know And How To Keep Your Data As Safe As Possible,"* Forbes.

[105] Lovett, L (September 18th 2020) *"FemTech players call out Facebook for rejecting women's health ads,"* MobileHealth News and Smith, B (June 8th 2023) *"Facebook removes sanitary towel ad for saying 'vagina',"* The Telegraph.

[106] See, Meta for Developers, "*Meta Pixel-Documentation*."

[107] See, Das, S (May 27th 2023) "*NHS data breach: trusts shared patient details with Facebook without consent,*" The Guardian and Das, S (June 3rd 2023) *"UK mental health charities handed sensitive data to Facebook for targeted ads,"* The Guardian and Das, S (July 15th 2023) *"Revealed: Metropolitan police shared sensitive data about crime victims with Facebook,"* The Guardian.

[108] The FTC Office of Technology (March 16th 2023) *"Lurking Beneath the Surface: Hidden Impacts of Pixel Tracking."*

[109] FTC, For Your Information (June 22nd 2021) *"FTC Finalizes Order with Flo Health, a Fertility-Tracking App that Shared Sensitive Health Data with Facebook, Google, and Others."*

[110] Osberg, M and Mehrotra, D (February 19th 2020) *"The Spooky, Loosely Regulated World of Online Therapy,"* Jezebel.

[111] FTC Case No. 1:23-cv-3107 May 17th 2023 Easy Healthcare Corporation "*Complaint For Permanent Injunction, Civil Penalty Judgment, And Other Relief",* p17.

[112] FTC (May 17th 2023) *"Ovulation Tracking App Premom Will be Barred from Sharing Health Data for Advertising Under Proposed FTC Order,"* Press release.

[113] The Conversation (October 19th 2017) *"Nobody reads privacy policies – here's how to fix that."*

[114] Mehrnezhad,M and Almeida, T (2021).

[115] See, Rakova, B (January 10th 2023) *"Terms-we-Serve-with: Introducing a new mechanism for engaging with algorithmic systems,"* Mozilla blog and Terms-we-Serve-with.

[116] See Andrson, S (July 10th 2023) *"Attribution matters: how marketers are navigating an 'uncomfortably complex topic',"* The Drum and Green, R (March 4th 2022) *"Attribution is Overrated,"* Ad Exchanger and Langford, R (September 28th 2021) *"Google shakes up ad metrics: last-click attribution axed for new AI model,"* Performance Marketing World.

[117] Thomson, M (February 8th 2022) "*Privacy Preserving Attribution for Advertising,*" Mozilla blog.

[118] Cox, J (November 16th 2020) *"How the U.S. Military Buys Location Data from Ordinary Apps,"* Motherboard.

[119] Kelly, M.J (June 23rd 2020) *"Firefox Relay protects your email address from hackers and spammers,"* Mozilla blog.

[120] See, https://github.com/flohealth

Bibliography

Benjamin, R. (2019). Technology after Race. Cambridge: Polity Press.

Benjamin, R. (2022) Viral Justice. Oxford: Princeton University Press.

Citron, D.K. (2022). The Fight for Privacy: Protecting Dignity, Identity, and Love in the Digital Age. London: Penguin Random House.

Criado Perez, C. (2019). Invisible Women: Exposing Data Bias in a World Designed for Men. London: Penguin Random Press.

D'Ignazio, C., & Klein, L.F. (2020). Data Feminism. London: The MIT Press.

Haugen, F. (2023) The Power of One. Blowing the Whistle on Facebook. London: Hodder and Stoughton.

Higgs, J. (2019) The Future Starts Here. Adventures in the Twenty-First Century. London: Weidenfeld and Nicholson.

King, A. and Crewe, I. (2014) The Blunders of Our Governments. London: Oneworld Publications.

York, C (2020) Silicon Values. The Future of Free Speech Under Surveillance Capitalism. London: Verson

Zuboff, S. (2019) The Age of Surveillance Capitalism. The Fight for a Human Future at the New Frontier of Power. London: Profile Books Ltd.