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

Summary and Recommendations
October 2023
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.

See full report by Lucy Purdon, Senior Tech Policy Fellow at Mozilla Foundation.

Available at: foundation.mozilla.org/en/blog/
• 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.
Recommendations for Action

**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.

**For Policymakers: Priorities for Reform**
**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.
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.