TECH HIVE ADVISORY
aapti institute

A Call for Ethical Femtech:

Balancing innovation and responsibility

May 2023

Artist: Khyati Trehan
Cover Art Credit

About Tech Hive

Tech Hive Advisory Limited (“Tech Hive”) is a technology policy and advisory firm that provides advisory and support services to private and public organisations regarding the intersection between technology, business, and law. We focus on how emerging and disruptive technologies are altering and influencing the traditional way of doing things while acting as an innovation partner to our clients.

Our experience and capability extend across Research and Policy Advisory, Privacy and Data Protection, Data Ethics, Cybersecurity, Start-Up Advisory, and Digital Health. We ensure our advice serves our clients well by having an excellent understanding not only of their business but of the markets in which they operate through accurate policy and legislative development tracking and intelligence.

Contact: contact@techhiveadvisory.org.ng

About Aapti

Aapti is a global public research institute that focuses on the intersection of technology and society and works to build solutions that generate societal impact, justice and equity. Aapti's work is carried out through two labs: the Data Economy Lab, a space dedicated to shaping a responsible and rights-based data economy, and the Digital Public Lab which solves for inclusion, access and equity for digital transformations on the ground. This work spans many aspects of our digital lives - and involves research, developing and testing solutions, and embedding them in policy and within organisations to achieve scale.
Contact: contact@aapti.in

Authors

Amrita Nanda, Suha Mohamed, Sandra Musa, Tolulope Ogundele, and Victoria Adaramola

Disclaimer

The Guide is general and educational in nature and is not intended to provide, and should not be relied on, as a source of legal advice. This information and material provided in the Guide may not be applicable in all (or any) situations and should not be acted upon without specific legal advice based on particular circumstances. The absence of any trademark or service mark from this list does not waive Tech Hive’s intellectual property rights in that name, mark or logo.

Introduction

When considering the history of feminine health and the breadth of medical research on female physiologies and diagnostics, the field of view unfortunately does not extend very far. Androcentrism has been the foundation of years of medical research, situating men as the human "general", and women as a necessarily gendered deviation from that median. The result has been a now well-documented disadvantage for women's health - be it in research, diagnostics, cures, or, in many cases, a culture of direct dismissal of women's symptoms in clinical settings. This has left women's physiologies chronically under-researched and misunderstood, with serious consequences for the care, wellbeing, and visibility of women's health. A huge lever of this kind of invisibility is the lack of available, reliable, and verified data on key aspects of women's health. This is further pronounced in stigmatised aspects like reproductive, sexual, or menstrual health, which see a compounded erasure from societal disinclinations and discomfort around them, despite their incredible criticality to the lifecycle of human physiology. However, given data's role in invisibilisation, it also holds the potential to act as a tool for visibilisation - in increasing knowledge and autonomy.

The promise of Femtech

Here enters what has been termed the "Femtech Revolution.". The term typically refers to feminine health technology, usually apps or platforms, that may act as data generators and also as a site for users to gain a greater and more autonomous understanding of their menstrual, reproductive, or sexual health. While there is some degree of contention on whether we need to call out "women's" health as a subset or niche within healthcare, it has served as a convenient and pertinent designator for a long-ignored set within the universe of medical research. Overarchingly, proponents of 'Femtech' speak to its potential in addressing the gender data gaps in medical research while instilling participation and input from users in how their data is governed, shared, and used. This growth of Femtech applications have put women's health issues and research on the map, and has also seen enormous recognition and funding in recent years. It is projected that the Femtech market share will reach a share size of 50 billion USD by 2025, and currently, Femtech applications are the fourth most popular type of apps among adults and the second most popular type among female adults.

Issues and concerns around Femtech

The potential of Femtech to democratise, create systems of autonomy and greater knowledge and research is clear, and energising. But how this is panning out in practice does not always embody these notions. The overturning of the landmark Roe v. Wade judgement, which criminalises the right to abortion in the United States, sparked broader conversations on the leakage of personal health data from social platforms, period-tracking apps. In anticipation of the judgement, the calls for the deletion of period-tracking apps (many of which log the use of contraceptives, amongst myriad other data that may be used to glean an individual's reproductive choices) were not unfounded. One of these calls was a petition by a number of Google employees calling for Google to delete information about users who visit abortion clinics or other places that could trigger legal problems. The legacy of Femtech today reflects an astonishing number of privacy violation concerns.

These events served not just as a cautionary tale but revealed how the absence of a robust data protection framework and accountability mechanisms can directly lend itself to the violation of digital privacy and rights. This lack has real world implications for reproductive health and wellbeing - and more glaringly, threatens human rights, liberties, and freedoms. It similarly reflects the consequences of societal perceptions and moralistic assumptions on how digital and data-based systems are designed and governed.

Considering that access to reproductive rights and care is already fraught across the world due to offline barriers and breakdowns, these inequities are likely to be further threatened through the irresponsible collection, governance, and use of data. This turn of events was just one of many that highlight the need for both urgent thinking and the shaping of more just and responsible stewardship of data - particularly women's health data.

So, as critical as the turn toward addressing and democratising women's health research has been, the digital age brings with it a novel set of potential harms. Harms that, if not pre-empted or mitigated through design and regulation, can (and have already been found to) carry dangerous implications for communities that have already historically been disenfranchised. Heeding this call, Aapti Institute has partnered with TechHive to understand the emerging harms of 'femtech apps' and define a set of foundational components that encourage safer and more secure collection and stewardship of data. This piece is focused on "period-tracking apps," as we have observed that these command an increasingly large usership and collect data at a significant volume.

Possible harms and how they arise

Once considered a subset of healthcare, there has now been a rise in the availability of period-tracking apps which offer users the ability to log one's own symptoms, cycles, and progressive healthcare needs, combined with the promise of privacy. However, as detailed above, this equitable and transparent vision is not necessarily how the industry is evolving.

To start with, the data collection and governance practices of Femtech companies are often incongruent with users' privacy rights and health data security. Most Femtech companies operate devices outside the bounds of a regulatory framework. The lack of overarching privacy frameworks in most jurisdictions has also resulted in a wild west of privacy practices, where consumer privacy is an afterthought. Femtech companies have been found not to prioritise or emphasise user privacy and security, despite the sensitive nature of health and, more recently, genetic data they collect. This lack of priority is evident in the 2019 case involving 'Flo'. The fertility tracking app was alleged by the Federal Trade Commission (FTC) to have disclosed sensitive health information, such as a user's pregnancy, to third parties in the form of "app events" for various reasons and did not limit how third parties could use this shared data.

Data brokerage of reproductive health data is another issue that has become endemic to Femtech, where the monetization of health data has become central to many companies' business models. While it's likely that users are aware data is being gathered by these applications, dense privacy policies often obscure the realities of where and with whom this data is being shared with. In 2020, a study by the Norwegian Consumer Council examined ten popular Femtech apps, including Flo, and found that the apps were collectively transferring information to at least 135 third-party companies or data brokers. There are consequences of these sharing practices, even where data may have been de-identified by these companies. The risks of re-identification are still concerning, and users may be traced and identified where this data may be coupled with other personal or publicly available information.

Privacy and health data protection may be further strained in the wake of the Roe v. Wade decision. This decision has created a hostile environment for women and clogs the wheels of Femtech. With the recent reversal, Femtech companies may be able to disclose users' reproductive health data to law enforcement authorities to investigate and prosecute women who have had or plan to have abortions. This information may be obtained directly from femtech companies through subpoenas, as most privacy notices often permit data disclosure to law enforcement authorities for legitimate purposes and in response to subpoenas or legal requests, or directly from a woman's digital device or cloud storage. For example, in 2017, a woman in Mississippi was charged with second-degree murder for the death of her foetus after her cell phone data revealed internet searches related to the purchase of abortion pills. Also, there are concerns about an increase in the value of reproductive health data, and breaches or cyberattacks will significantly increase. Hackers and cybercriminals may gain access to or compromise Femtech applications or devices to steal health data and subsequently sell it on the dark web or use it to blackmail or extort companies and the women whose data they possess to make financial gains.

These are but a few examples of the kinds of harmful consequences we have begun to see. These realities are an important reminder that we need secure, responsive technologies built along feminist, privacy-centric principles that are accompanied by better accountable and transparent data governance models. Our early insights into the space have highlighted three key areas that can contribute to a more equitable ecosystem for Femtech and reproductive health research. ***Specifically, in privacy and ethics by design, in accountability through regulation, and in agency through alternative data governance (data stewardship).***

Building ecosystems of protection, transparency and agency

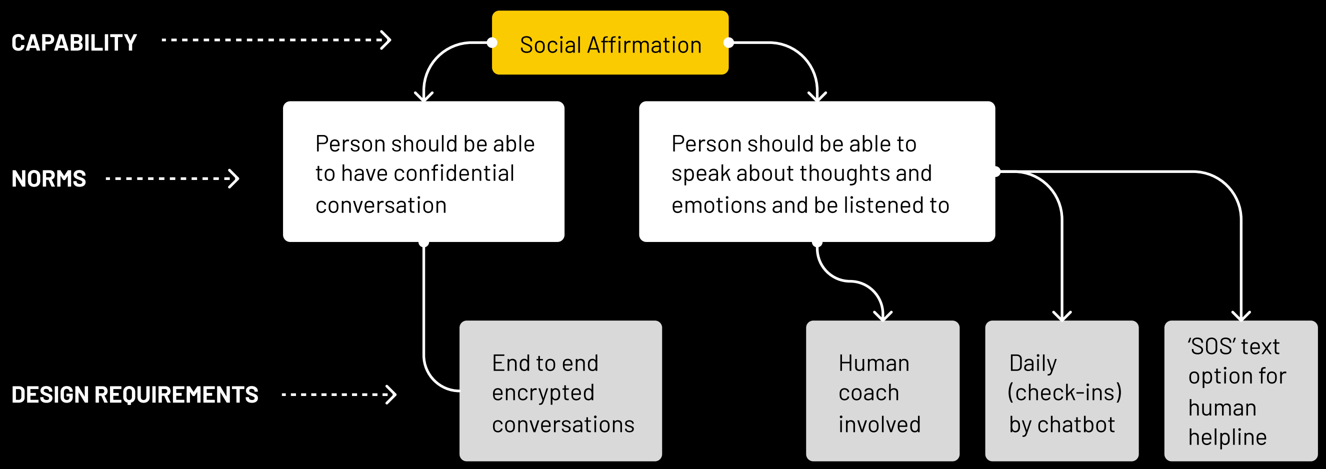
Building : Privacy & Ethics by Design

Data captured by femtech apps can unlock value at an individual and societal level, providing users with greater insight around their personal reproductive health/wellbeing and fill critical gaps in health and medical research. Ideally, this should take place within regulatory contours that safeguard the rights (online and offline) of data subjects. However, in the absence of coherent protections or where diverging regulations do not impose necessary safeguards, developers must also shoulder responsibility and consider how to instantiate 'privacy by design' within femtech applications.

Privacy by design is often interpreted as a set of ethical, design, technical and governance practices which nudges developers to "actively design for values". While varied techniques exist to instantiate privacy by design into practice, fewer frameworks focus on its connected praxis, ethics-by-design. To address this, scholars have specifically pointed to Capability Sensitive Design (CSD)' as a particularly relevant normative framework to 'evaluate the design of health and wellbeing technologies'. CSD is rooted in Nussbaum's capabilities approach and therefore encourages ethicists and designers to think holistically about how technology can enhance what people 'are able to be and do'. Put simply, capabilities can be defined as freedoms and self-described opportunities - while Nussbaum's theory lists ten, other scholars believe this should be interpreted more broadly and be defined in a more participative manner. Capabilities are defined in conjunction with 'functionings' that describe the actual realities of what people experience and are faced with.

Lastly, this framework also introduces 'conversion factors' that can be personal (internal dimensions - physical condition, intelligence etc), social (norms, public policies, power dynamics etc) and environmental (related to the physical & built environment). These conversion factors influence the extent to which resources can be transformed into 'functionings'. To translate these abstract conceptions into tangible design practices, scholars have suggested adopting the 'capability hierarchy' tool. An illustration of how this tool has been applied by Jacob (2020) in the design of a mental health chatbot is illustrated in the figure below:

Figure 1: Capability Hierarchy applied in context of a mental health chat tool


CAPABILITY
Social Affirmation
NORMS
Person should be able to have confidential conversation
Person should be able to speak about thoughts and emotions and be listened to
DESIGN REQUIREMENTS
End to end encrypted conversations
Human coach involved
Daily (check-ins) by chatbot
'SOS' text option for human helpline

While not a traditional design tool, this hierarchy chart can help tease out potential end user 'capabilities' and how these may intersect with norms and possible design requirements. Alternatively, Classen (2011), suggests a more participatory data gathering approach to nuance end-user needs and capabilities framings through a 'philosopher-investigator' approach. This strategy encourages understanding what capabilities people value the most, instead of assuming these directly. Co-design sessions that involve end-users in the consultation, prototyping and deployment of applications can be a bottom-up strategy of highlighting these 'capabilities'. UNICEF's Oky app, a period-tracking app for young menstruators, was designed with this logic in mind - teams engaged with girls in Indonesia and Mongolia to better understand usage, needs and interests for the app. UNICEF's team was cognisant of cultural nuances as well as unique 'social norms' like shared phone usage in family settings, and built related privacy features like individual log-ins and ensured data was stored locally devices to allow private and confidential use for period-tracking. In a similar vein, they considered 'environmental factors' like the girls' access to bandwidth and low connectivity settings, and designed the app to be available in offline settings.

In addition to these participatory approaches, privacy-by-design practitioners also recommend a set of core governance practices that can be encoded into the design of femtech apps. Many of these principles draw from regulations like GDPR which articulate data users' rights to access, delete and have portability around their data, but also encourage the 'minimization' principle around the collection of data.
While minimisation is an important foundational principle, it must be nuanced in interpretation and balanced with the need to responsibly capture data - to address gender data scarcity concerns or improve inclusion and diversity in clinical research in order to better serve unique healthcare needs of women and other sexual and gender minorities. An agential read of these privacy practices, imagines a broad set of capabilities and associated design requirements. For instance, it's possible that a woman diagnosed with endometriosis would like to be a part of data gathering efforts to contribute towards capabilities or opportunities that include 'having good health', while 'maintaining bodily integrity'. The normative orientation could therefore be framed as 'users can be active participants in the data collection and research journey', and 'users should be able to privately and securely track, manage and understand their data'. Citizen Endo, an initiative launched by Noémie Elhadad, a professor at Columbia University, created the Phendo App with these considerations in mind. Therefore, design requirements and governance principles that could follow may include: 'Showcase personalised and collective insights to users', 'provide users with an accessible feedback loop for participants to stay actively connected with research outcomes'. Flowing from these normative and design propositions, a number of technical practices like encryption and local storage of data on devices can additionally be put in place. Applications like Drip, described as ***'an open-source cycle tracking app that keeps your data private and on your phone***', have designed their collection and governance of data with participation, transparency and security as core tenets. Local device storage as a security mechanism is highlighted as a central aspect of their data governance as well as their value proposition to their potential user community.

In a similar vein, Clue, which has committed itself to a business model that is not data monetization driven, but rather one that centres privacy, has developed accessible messaging for users who want to learn more on which third-parties they share data with and 'what happens to your tracked data' . For context, Clue engages with research partners to further knowledge building on menstrual and reproductive health - data gathering may sometimes go towards this goal or be used for product-level app design improvements. Additionally, Clue provides users with the ability to easily opt-out of any form of tracking, advert, and restrict forms of processing in the best interest of their privacy through an in-app toggle.

Whether through data governance practices, in-app design or participatory data collection efforts - privacy and ethics by design must be developed in a context specific and community-oriented way. Creativity can be exercised in understanding how to best frame what user 'capabilities' can be prioritised and designed for, while accounting for personal, social and environmental conversion factors. For femtech app developers seeking immediate and actionable steps, a starting point may be to explore the American Medical Associations 'checklist for app developers', part of their publication on 'Privacy is Good Business: A case for privacy by design in app development'

Policy : Regulatory moves that can help

Femtech apps, as discussed, collect diverse and useful data from a huge number of users while providing sometimes inadequate safeguards for the protection of the data collected. While each jurisdiction governs data rights and protections in unique ways, which, for most, are still evolving - there exist certain pathways that can be considered par for the course in how they enable the protection of Femtech users and data providers. In an ideal scenario, we would see a global standard for the protection, management, and use of sensitive data. But in the absence of such standards, there is great potential to identify and promote diverse regulatory pathways in various jurisdictions, which can enable greater transparency and, crucially, accountability in the building, deployment, and use of Femtech.

Regulatory boundaries must focus on protecting the privacy of users while ensuring that their consumer rights are protected. There is also potential for healthcare laws to include confidentiality between applications and users, based on similar principles as doctor-patient confidentiality - which finds mention almost entirely across the globe. In the case of data, these kinds of confidentiality frameworks need to be bolstered by a specific focus on the nuances of data storage, retention, and anonymisation in cases where user data may be used for research.

While there are a number of regulations that touch upon these kinds of data, there is significant scope for improvement. In the United States, the site of heated debate around abortion laws, HIPAA governs how much medical/health information can be shared by caregivers and to what ends. Under its provisions, doctors or medical organisations can share sensitive personal health information if they believe a crime has been committed. It also doesn't apply to all the groups or entities actually providing medical care to citizens, such as crisis pregnancy centres. For countries in the global south, the United States sets a dangerous precedent of regulation that may miss the nuances and pronounced harms of digitalised healthcare information. Globally, there is a need to build privacy, agency and safeguards against the misuse of data arising from Femtech - in a manner that responds to the digital experiences of women and gender minorities. A potential pathway may be to frame these rights as an offshoot of reproductive rights. This is particularly viable for countries that already house mature protection around reproductive rights. In such cases, there may be scope to include these protections under the 'right to privacy' but they may also be located within wider frameworks (constitutional or otherwise) of substantive equality.

These are some of the challenges and solutions to substantially governing Femtech data. However, data and data governance present a novel challenge, one that can be approached by policymakers with a view to not only building equitable systems going forward but also as a chance to rewrite existing inequalities within society. Femtech, in particular, presents this chance.

Alternative forms of data governance : Data Stewardship for Femtech

As highlighted in the privacy and ethics by design discourse, data governance can play a fundamental role in enabling more agency, transparency and control over data in femtech. While this can be supported by top-down regulatory mechanisms, it must in parallel be supported by bottom-up efforts. Data stewardship, a paradigm proposed by Aapti Institute, seeks to create greater agency and negotiating power for data subjects while unlocking the social value of data. It imagines strengthening and empowering 'stewards' or data-institutions (for e.g advocacy organisations, femtech developers, multilateral institutions, non-profits, social enterprises, development agencies) which act with a duty of care towards their beneficiaries, and can operationalise their responsibility to safeguard digital rights through a set of technical, governance-oriented and community-centric practices.

Data stewards are entities that are typically well-rooted in the communities they support, often possess technical expertise, and critically support 'data subjects' by negotiating and advocating on behalf of communities and individuals, with data requesters or data holders, who are systemically and epistemically in positions of greater power. Furthermore, empowering trusted stewards in contexts with highly sensitive data that belong to vulnerable and marginalised communities, may be beneficial as they may be best placed to envision pathways of value from data that serve to unlock the societal benefits of data. This is not always something communities are able to do alone or have the bandwidth for.

For instance, another period-tracking app, Euki mentions it 'helps you get answers that you can trust without making assumptions about who you are, what you do or don't already know, or how you identify." The app has also been designed to safeguard security and privacy of data by storing information locally on devices, and provides alternative security mechanisms.

This piece has already highlighted several organisations that could be defined as 'stewards' in their own right - organisations often run by women and other gender minorities, oriented on the basis of feminist and ethical principles - that are building tech by and for their own communities. For instance, Clue and Drip both communicate their responsibility and related organisational structure and practices they adopt to both unlock the value of data while safeguarding rights. Similarly participation in governance and co-design are a significant part of both organisations' ethos, although reflected in different modalities. Drip, specifically, has been designed as an 'open-source, non-commercial, gender inclusive, secure, science based' app that relies on the sympto-thermal method of data gathering for fertility/period-tracking. Developed by the Berlin based 'Bloody Health' collective and hosted on GitHub, it has been kept running by a community of dedicated contributors.

Part of the journey towards empowering these 'stewards' are to identify models by which they can continue to operate sustainably in service of their communities - without engaging in data surveillance, monetization or exploitation of any means. As articulated by GenderIT "The feminist internet movement needs funding but make no mistake - we (funders, users and consumers) need it more than it needs us.". To address funding disparities in health research and diversify sources of capital, Clue has recently opened up a crowdfunding campaign, where for 10 euros or upwards, users can become co-owners with equity, enabling them to take part and be privy to product development, innovation and financing health research or addressing gender data gaps in menstrual and reproductive health.

While the space for alternative solutions to the dilemmas of Femtech is still being explored, data stewardship can certainly form one piece of the puzzle. They must be deployed in conjunction with (in some cases, stewards can specifically catalyse) privacy by design, regulatory protections, and multi-stakeholder accountability mechanisms.

Conclusion and looking forward

With the clearly increased risk of women's sensitive female health data becoming shareable commodities, Femtech or healthtech apps may be becoming counterproductive at best and deeply damaging at worst. This poses a major challenge to women's health, safety and digital rights. This puts us at a critical juncture - one at which research, policy, and design must all coalesce around the prioritisation of safety, agency, and meaningful community value from the adoption and inevitable growth of Femtech. The ecosystem of Femtech must begin to prioritise the principle of transparency with their users about the data they collect as well as the methods they use to collect it. Stewarding entities dedicated to collecting and sharing reproductive and menstrual health data must continue to explore pathways for representation, transparency, and participation in building, deploying, and governing the data they collect or have access to. Moreover, the existing ecosystem around Femtech, across each layer of stakeholders, whether academia, builders, funders, advocacy, or more - must come together to prioritise the privacy of Femtech users.

techhiveadvisory.africa | aapti.in

TECH HIVE ADVISORY aapti institute