GENDER OPEN REPOSITORIUM

Refusing Platform Promises : A Gendered Rewriting of Digital Imaginaries

Shah, Nishant

2023

https://doi.org/10.25595/2298

Veröffentlichungsversion / published version
Zeitschriftenartikel / journal article

Empfohlene Zitierung / Suggested Citation:

Shah, Nishant: *Refusing Platform Promises : A Gendered Rewriting of Digital Imaginaries*, in: Open Gender Journal, Jg. 7 (2023). DOI: https://doi.org/10.25595/2298.

Erstmalig hier erschienen / Initial publication here: https://doi.org/10.17169/ogj.2023.214

Nutzungsbedingungen:

Dieser Text wird unter einer CC BY 4.0 Lizenz (Namensnennung) zur Verfügung gestellt. Nähere Auskünfte zu dieser Lizenz finden Sie hier:

https://creativecommons.org/licenses/by/4.0/deed.de

Terms of use:

This document is made available under a CC BY 4.0 License (Attribution). For more information see:

https://creativecommons.org/licenses/by/4.0/deed.en

GenderOpen – Repositorium für die Geschlechterforschung: www.genderopen.de

FREIE UNIVERSITÄT BERLIN

HUMBOLDT-UNIVERSITÄT ZU BERLIN

OPEN GENDER JOURNAL

Refusing Platform Promises. A Gendered Rewriting of Digital Imaginaries

Nishant Shah (nishantshah@cuhk.edu.hk)

Abstract: Platforms have recently come under scrutiny, both in policy and in scholarship. Yet, there is little attention paid to the notion and materiality of gendered practices. Although gender is present on these platforms, it is not necessarily endemic or critical to the analysis of these platformed practices. Platform Promises is a way by which we look at platformisation of gender, focusing on how gender politics are coded into the logic and infrastructure of these platforms. I propose that we stop thinking about platforms as technological engineering artefacts upon which conditions of gender are operationalised. This framing makes us believe that gendered and sexual violence online are a state of exception which can be fixed through better regulation and governance. I propose that we use gender as both a discursive and an analytic category by which to rewrite the discourse on platforms, to see the platform promises that are taken for granted and are not questioned in the dominant narratives.

Keywords: Digital Cultures, Digital Platforms, Social Media, Violence against Women

Submitted: 19. August 2022
Accepted: 17. March 2023
Published: 27. October 2023

Cite as: Shah, Nishant (2023): Refusing Platform Promises. A Gendered Rewriting of Digital Imaginaries. In: Open Gender Journal 7. doi: 10.17169/ogj.2023.214

DOI: https://doi.org/10.17169/ogj.2023.214

Edited by Katrin Köppert, Sara Morais dos Santos Bruss and Maria Haeusl

Creative Commons Attribution 4.0 International

Nishant Shah

Refusing Platform Promises. A Gendered Rewriting of Digital Imaginaries

Platforming Gender

Digital platforms such as Facebook and Instagram have rightfully come under increased scrutiny recently, both in policy as well as in scholarship. One of the most significant approaches to understanding platforms is through the framework of "platformisation" by Thomas Poell, David Nieborg, and José van Dijck (2019). Identifying the digital platform as a historical, polyvocal, and multimodal concept that draws from different genealogies of technology development and technocultural practices, their essay offers a distinct shift from the study of platforms to "the (re-)organization of cultural practices around platforms, while these practices simultaneously shape a platform's institutional dimensions" (Poell/Nieborg/van Dijck 2019, 1). They offer a compelling synthesis of platforms along the three institutional dimensions of "data infrastructures, markets, and governance" (ibid., 6). This significant framework brings in the critical work of digital-methods-studies scholars such as Anne Helmond (2015), who has shown the ways in which the rhetoric of decentralisation of platforms accompanies the "recentralization of 'platform ready' data", which has dire consequences for the programmability of social media platforms. This builds on the historical work of media theorist Tarleton Gillespie (2017), who begins with the platform as a metaphor before examining the material consequences of this idea for expanding economies of exploitation at a scale-free level. This thesis also brings in emerging critical frameworks from infrastructure studies and platform studies to critique digital information giants like Facebook and Google. Such work also strengthens the legacy arguments of technology-labour scholar Trebor Scholz (2016), who, in his proposition of "platform cooperativism", offers a community-driven approach to ownership and the possibility of harnessing what Yochai Benkler (2006) once fondly called "the wealth of networks".

All this work on platforms, platformisation, and platforming of digital technologies through infrastructures, markets, labour, governance, programming, design, and policy provides valuable insights into thinking through the possibilities, paradoxes, and contraries of studying and staying with the platforms

rather than just seeking to replace or reject them. And yet, there is very little attention paid to the notion and materiality of gendered practices and lives in these discussions. When gender does appear in platform studies, it is mobilised in terms of economic categories of labour and production, political values of access and ownership, governance structures of redress and justice, or cultural practices of representation and creation. Gender rides, resides, and leaves residue on these platforms, but it is not necessarily something that is endemic to the study of or critical to the analysis of these platformed practices.

In October 2021, former Facebook employee Frances Haugen revealed to the world that the two biggest social media platforms – Facebook and Instagram – had deliberately incentivised, programmed, and platformed violence against women on their sites. Invoking the perpetual figure of concern online – children, especially young girls –, Haugen justified her presence with a powerful opening: "I'm here today because I believe Facebook's products harm children, stoke division, and weaken our democracy" (Haugen 2021, 1).

In Haugen's testimony, the harm that Facebook and Instagram cause to young women, making them "feel bad about their bodies", is described as avoidable and reversible. Haugen states,

> "The company's leadership knows how to make Facebook and Instagram safer, but won't make the necessary changes because they put their astronomical profits before people." (ibid.)

In her capacity of lead product manager for civic misinformation and later for counter-espionage, she "saw that Facebook repeatedly encountered conflicts between its own profits and our safety. Facebook *consistently* resolved those conflicts in favour of its own profits" (ibid., 2; my emphasis) and revealed with authority that "their profit optimizing machine is generating self-harm and self-hate – especially for vulnerable groups, like teenage girls" (ibid.).

However, Haugen was not just a whistle-blower. As somebody who had experienced the company's "infinite resources" (ibid.), she provided suggestions to diminish and decrease this harm, which Facebook is currently aware of but not addressing. In particular, Haugen claims that the "core of the issue is that no one can understand Facebook's destructive choices better than Facebook, because only Facebook gets to look under the hood" (ibid.), which is why she calls for transparency as a critical starting point for effective regulation.

Haugen has stated that her testimony was to establish conditions of accountability in order to ensure that Facebook be regulated to stop making choices that go against the common good – "*Our common good*" (ibid.; her emphasis). Further incriminating Facebook's own constitution of its oversight board, she insists that the board is "as blind as the public" (ibid., 3). She claims that right now,

there is no independent assessment of Facebook, and our only relationship with the platform is one of "blind faith" (Haugen 2021, 3). This way, we are being made to believe that we have to choose between connecting those we love online and our personal privacy. This naturalises the idea that in order to share our personal memories, we have to be "inundated with misinformation" (ibid., 4).

Haugen's testimony is brave, powerful, poignant; it has held the collective global attention on the harms of social media practices. There is renewed interest now not only in revealing the ills of companies that profit off managing human relationships but also in stopping their spread. There is no denying the personal and professional risk that Haugen took in stepping forward to, ironically, tell us something we had already known – or at least suspected. This revelation of that which we already knew is perhaps the moment of puzzlement that can help us ask what it was that was so extraordinary about Haugen's testimony, because none of this is particularly new. Feminist scholars and activists who have been working on online gender-based violence have long documented and deplored the lack of oversight, redress, accountability, and protection when it comes to women's presence, voices, and bodies online. Similar concerns have been voiced by scholars and activists in queer and trans communities, who have seen the conditions of social harm and self-harm that vulnerable groups are subjected to.

In 2017, the Association of Progressive Communication (APC) submitted a comprehensive report on online gender-based violence to the United Nations Special Rapporteur, in which the authors clearly state,

> "In the digital age, the normalisation of violent behaviour and the culture that tolerates violence against women that social media perpetuates and facilitates at rapid speed, work to reinforce sexist and violent attitudes, and contribute to norms and practices that make online and offline spaces hostile towards women and communities most at risk of injustice and indoctrination." (Association for Progressive Communications 2017, 4)

This report draws from many years of previous work that consistently shows this dangerous condition. Similarly, Namita Malhotra's comprehensive report on social media companies clearly spells out that companies such as Facebook do only the minimum required by law to protect women on their platforms (2015, 5), and that when necessary, they are able to perform ad hoc acts of censorship and removing data. Malhotra refers to Facebook's repeated decisions to remove pictures of breastfeeding mothers while continuing to allow images that are more graphic and often violent towards women (ibid., 8). She also shows how in many other geographies, particularly in Europe with its data

protection authorities, Facebook's terms of service are seen as questionable and have led to calls for accountability (Kayyali 2015).

There has also been scholarship focused on non-consensual sharing of pornographic images. In my own work (Shah 2016), I showed how networked logics promote and champion the circulation of harmful images, overriding the consent and agency of the women affected by these weaponised protocol practices. During the same time, Wendy Hui Kyong Chun and Sarah Friedland produced a powerful analysis of how social media companies such as Facebook and Instagram were complicit in "habits of leaking"[1] (2015) as they circulated images and responses leading to the tragic death by suicide of 15-year-old Canadian student Amanda Todd.

Elizabeth Losh's powerful retelling and analysis of the #Gamergate controversies (2016) shows the affective construction of violence and the ready-to-deploy weaponisation of hatred for women online. Looking at the ways in which feminist game developers Zoë Quinn and Brianna Wu as well as cultural critic Anita Sarkeesian were harassed, doxed, and threatened for their calling out misogyny in online gaming cultures, Losh is quick to remind us, using Julian Dibbell's (1993) landmark essay on how "rape happened in cyberspace" that "online misogyny and gender-based aggression have had a long history in digital culture that goes back to bulletin boards, MOOs, and MUDs and the existence of virtual rape in early forms of cyberspace" (Losh 2016, paragraph 17).

Before Haugen's testimony received public attention, Neema Iyer, Bonnita Nyamwire, and Sandra Nabulega had already published their interactive "survival guide to being a woman on the internet"[2], followed by their report "Alternate Realities, Alternate Internets", in which they show that a "majority (71.2%) of all the incidents of online gender-based violence against the respondents occurred on Facebook. In Kenya, Uganda, Senegal and South Africa, this violence primarily happens on Facebook and WhatsApp" (2020, 24), with Instagram in a close third place. These are not just the globally prevalent social media networks but products owned by their shared parent company, Facebook (now rebranded as Meta). Iyer, Naymwire, and Nabulega show through detailed interviews and testimonies that women in public spaces, women in social settings, and women in domestic conditions experience threats of violence and conditions of abuse through trolling, doxing, and lack of support from the respective social media

1 The concept of habitual leaking, as introduced by Chun and Friedland has been powerful in thinking about the ways in which we habituate our leaking of data in everyday digital transactions, no longer paying attention to it, but also how our consent at leaking data is habituated by the design of digital technologies and practices.

2 This interactive platform is accessible at https://ogbv.pollicy.org.

platforms, only to be given the advice to disengage or self-censor in order to keep themselves safe.

This is not a comprehensive or an exhaustive account. However, such repeated reports, often from women, queer and trans-rights activists, and scholars in non-canonical geographies of the internet, present an indicative snapshot of corporations' weaponising information to harm, hurt, intimidate, and erase women and gender non-conforming people in their networks.

It is in this light that I go back to the testimony of Francis Haugen and to why it became a landmark moment. Haugen did not merely say that gender was one of the sites of exploitation; she claimed that the production, circulation, manipulation, and distortion of gender and sexual bodies and their images were at the core of these platforms' structures. In Haugen's testimony, gender is not just something that is studied on the platform; instead, like infrastructure, data, code, programming, technology, and governance, it becomes a central trope through which platforms are operationalised, governed, managed, maintained, and sustained. Exploiting and targeting specific gendered bodies is a part of these platforms' core business, not just an unhappy coincidence. Online gender-based violence, which is endemic to these platforms, is, as the meme goes, not a bug but a feature.

Haugen's testimony, while powerful, is only an echo of what other voices have been talking about and fighting for for a long time. Perhaps because these other voices came from bodies that were non-normative and not occupying geographies of power or because they were from spaces and communities about which the global audience outraged by Frances Haugen's revelations did not care enough, they have not been given enough attention. The intersections of race, gender, geography, and technology have been well-studied, and it has been demonstrated that when people of colour or those from less influential groups point towards a problem, it is generally seen as a local problem the responsibilities for which are put upon themselves. The technology is "clean"; it is the people who are "dirty" and need to be rehabilitated into better behaviour (Zakaria 2021).

While I take the critique of social media platforms such as Facebook and Instagram as my starting point, this paper is not restricted to social media platforms only. Instead, I look at three different characteristics of platforms to elucidate the promises through which they justify their practices. The first case study looks at a web of social media platforms and the ways in which they can replicate scaled violence. The second case study examines what happens when the same platform offers multiple services, leading to centralisation of data-

bases that can override user consent and agency. The last case study looks at a government-owned platform and shows how new measures are installed for the verification of individuals and the consequences of failing these demands for verification. Through these case studies, I hope to identify the promises that justify the platformisation of gender and offer new categories that can rewrite these promises, demanding a recalibration of these platforms rather than just improving their scope of operations.

Platform Promises

My proposition is that while Frances Haugen's critique is sharp and astute in her analysis of the platformed machinery of hate and violence, her resolution, unlike other activist demands for radical reconstruction, is feasible and palatable. Even as Haugen uses the figure of the young women as the trigger point (along with radicalisation and polarisation) in her call for better regulation, eventually, her solution of accountability is embedded in a longer tradition of "radical transparency", which has long been heralded as the answer to most online gender-based violence. Effective transparency, demanding independent oversight, non-partisan research on these practices, and democratisation of their decision-making practices all, eventually, feed the promises of platforms. They are interventions that might reform the platforms but do not reject or even disrupt the imaginaries and promises that they have naturalised as the de facto ways of being digital.

Haugen's resolutions – which are largely technological – indeed fall back on these existing discourses of platformisation and platform studies. The logical next steps would be towards a reform of implementation, oversight of principles, and regulation of policies; steps that are already in operation without necessarily leading to accountable change, which, at its very best, is post-facto. However, her authoritative insistence from the inside on gender-based violence as the central guiding principle of favouring profits over protection is significant and allows us to look at the promises that platforms make, which critical platform studies might be able to resist if they understand gender (and its material, cultural, political operations) as central to understanding platforms.

I propose "platform promises" as a way to look at the platformisation of gender so that we shift our focus from the presence of gendered bodies on online platforms to how gender politics are coded into the very logic and infrastructure of these platforms. Using gender as a toolkit to unbox platforms, I propose that we stop thinking about platforms as technological engineering artefacts upon which social and political conditions of gender are operationalised. This framing

has enabled a narrative of "people doing bad things on good platforms" and presents platforms as agnostic and neutral to the practices of online gender-based violence. It makes us believe that gendered and sexual violence online is a state of exception that can be fixed through better regulation and governance.

I propose that we use gender as both a discursive and an analytic category by which to rewrite the discourse on platforms, to make visible the platform promises that are taken for granted and are not questioned in the dominant narratives on platforms. Gender, then, is not an example, site, or case study for illustration, but in fact a toolkit that helps scry platform promises and that also rewrites them by looking at bodily safety at the centre of the platformisation discourse. I do not attempt to offer an exhaustive set of principles for this gendered unboxing, but I examine three promises that need to be rewritten in order to engender platforms towards the "Feminist Principles of the Internet" (Association for Progressive Communications 2016).

Undeniability of Scale

The promise of networked digitalisation is scale. Digitalisation, especially in ICT4D[3] projects, is offered and justified in order to produce scaled access, distribution, and reach. The idea that we will be able to reach across the globe, into millions of nodes of information, all connected by the sheer joy of sharing information, has been very seductive in selling the narrative of expansion of digital networks. Platforms find their emergence in these imaginations of scale, valuing traffic, engagement, circulation, and spread as the currency of "digital liveness" (Auslander 2012) and robustness. It is not a surprise that scale is the life blood of digital platforms. The rise of virality and influencer cultures (Abidin 2018), memetic replication (Arkenbout/Wilson/de Zeeuw 2021), and scale-free systems of circulation are all examples of how scale has become the default mode of evaluating and measuring digital life and being. Corporate and marketing mantras that have hinged themselves onto "big data futures" (Wang 2013) continue to reiterate that the premise and promise of all digital communication is scale, and information that does not lend itself to sharing, is information that is dead.

It is interesting that in a post-Cambridge-Analytica world, we still need to understand the dark side of sharing, and particularly, how this unfettered idea of sharing is modelled almost entirely on gendered harm. One of the most illustrative cases that exemplifies this is a controversy that emerged in India, in the

3 Information and communications technology for development.

midst of the global COVID-19 pandemic, during which a large part of sociality shifted online. In July 2021, an open-source app called Sulli Deals went viral in India (Pandey 2021). Created by a Trad group[4], Sulli Deals posted pictures and personal information of Muslim women online, each profile presented as "deal of the day" (Dutta 2022), open for a mock auction, where potential buyers were invited to express extreme Islamophobic, misogynist, violent, and abusive fantasies of what they would do to these women, collectively creating expressions and intentions of mass violence and abuse.

In January 2022, Aumkareshwar Thakur, identified as the creator of Sulli Deals, was arrested by the Delhi Police. After multiple attempts, the app was taken down from the Microsoft-owned open-code commons Github, where the app had been hosted (Sinha/Siddique 2022) and the account that hosted the app was deleted (Ramesh 2021). While these technological interventions were made and the platform was "debunked", the harm the app had caused was seen not as scalar but as individual. It remains a persistent trope in gender technology governance that while the visions and imaginaries of digital technology are presented in scalar matrices, its harm is not measured as compounded effects.

Feminist mathematician Cathy O'Neil (2016) points out that scale is not only the aspiration but also the justification for how our networks work. Because scale is the primary reason given for the networks, interventions that can stop potential harm caused by such networked apps and platforms also need to be at scale. Albert-László Barabási (2002) makes a similar argument by explaining that the measure of a computational system has to be in computational terms. Sulli Deals was not just an app gone wrong, an exceptional case. While the app was removed from Github, and while Twitter eventually suspended the respective accounts, it is important to realise that the harm the app had caused was long-lasting and intense.

Computational scale is not just about big data, which deals with the volume and velocity of information spread. In the expanse and speed of data sharing, human scales are disregarded in the equation. If we see digital data as *merely digital*, we forget that it affects human users, who are often not offered support, redress, or mitigation in the face of scaled-up violence. Scalar technologies create a disconnection between the lived experience of informational violence and the circulation of violence information, reducing the scope of mitigation on technology governance and platform regulation.

4 "Trad" is the moniker adopted by traditionalist groups on Twitter and Reddit that identify themselves as vigilantes and protectors of traditional values against progressive or liberal critique and transformation. Trad groups typically express high degree of misogyny, caste and race supremacy narratives, homophobia, and anti-migrant attitudes, among others.

Platforms depend on algorithm-driven computational scaling, creating instant copies and enabling simultaneous spread of information that cannot be controlled by individual regulations. Hence, when Haugen demands that Facebook and Instagram be regulated not as independent and discrete platforms but as symptomatic issues of a larger ecosystem of violence that will continue beyond individual accountability of these platforms, we need to pay attention.

Regulating technological scale through human experience and making human-sized interventions in stopping the spread of information is an exercise in redundancy. Sulli Deals is a clear example that scale is not only inherently desirable but often propelled by circulation of violence and abuse that is difficult to govern. The Indian government and authorities did eventually identify and convict the main developers and administrators of Sulli Deals. The app was pulled from circulation. The data about the Muslim women were erased from it. And yet, less than a month later, another app – Bulli Bai – was published that used Sulli Deals' open-source code and platform mechanics from Github, replicating the entire database and process (Salim 2022).

I am suggesting, then, that we rewrite the promise of scale, which necessarily exploits gendered hatred and violence, with measures of intensity. Intensity disrupts the promise of scale in two ways: First, it insists that conditions of harm do not have to be expansive for regulation to happen. Even when violence and abuse of harmful information is targeted at small numbers, they need to be taken seriously and immediately acted upon. Second, it offers us a different way of thinking about scalar regulations, demanding that the intensity that comes from attacks on safety, dignity, freedom, and liberty be taken seriously in these platformisations of gender, and that interventions cannot be limited to individual redress or brand-specific platform accountability; a complete recalibration of networked platforms is needed.

As Anna Lowenhaupt Tsing, in her proposition on "nonscalability", points out, "scalability is not necessarily a desirable promise" (Tsing 2012, 523). Looking at the history of colonial exploitations and extractions, she argues that scale "is not a necessary feature of the world" (ibid., 524). However, the antidote to scale is not nonscalability, which is also exploited by "supply-chain capitalism, from software to mining" (ibid., 521). Scale converts people into data. Intensity demands that this data become embodied again. In this embodiment, it refuses to evaluate the wellness of the network or the redress of the body as scalar mechanisms. Instead, it favours smaller, self-contained networks, which can be open to connectivity but are more in control of the scale of access and reach, demanding new conditions of embodied governance for platforms and their regulation.

Imperative of Interactivity

Scale is the promise of platforms and interactivity is the premise for platformisation. The rush to put everything onto platforms, creating specific, targeted, data-driven customisations for the "gig economy" have placed interactivity among different elements, shaping (or manipulating) them in order to create particular "network neighbourhoods" (Chun 2021), which have been the mainstay of platformisation. However, interactivity is not merely the ability to interact with different elements. In the interactive Web 2.0 environments that we have now naturalised, interactivity is transactability.

Human-rights and technology lawyer Kelly Kim, in her work on South Korea, argues for this, with her powerful statement that "the history of data protection in South Korea is a history of data breaches" (2020, 13). Kim reconstructs a specific case of data sharing that looks benign under the lens of interactivity but belies its intended breach of privacy when it is understood as transactability. Kim introduces the case of an artificial intelligence chatbot called Lee Luda. Lee Luda was an AI chatbot service developed in December 2020 by Scatter Lab in Seoul. It had a gendered, anthropomorphised presence and created the virtual profile of a 20-year-old female college student who introduced herself to the world with the tag line, "Hi, I'm your first AI friend, Lee Luda". People could add the bot to their social media, chat with it on Facebook Messenger, and have long (written) conversations with it. There was an immediate initial excitement that Lee Luda's conversations were natural, human-like, and engaging, and the bot generated more than 400,000 subscribers in the first two weeks after its launch.

However, two problems quickly arose. Lee Luda was being trained on a public conversation data set, thus mimicking and inheriting expressions of violence, discrimination, and hate speech against women, queer people, and other minorities. The unchecked training set amplified the bot's misogyny, which, once again, made gender-based violence the premise of expansion and scalar circulation. Additionally, because Lee Luda was having customised conversations with profiles that were not anonymous but clearly mapped to real-life users, it started directing its conversations only at specific user types, keeping its more public image clean and benign.

The second problem was even more difficult. Lee Luda was also being trained with another data set, one that contained private information that Scatter Lab had collected from its users via its other services. Lee Luda was not only learning and internalising that private information but also harvesting new information to fill in any empty fields through its interactions with new users. In this process, Lee Luda started leaking real life information – personal addresses, phone numbers,

health records, employment histories, etc. (Kim 2020, 17). This was information that users had given to another service by the company, but the same dataset was now being leaked into new application for which users had not consented to provide their data.

Anonymous users interacting with Lee Luda suddenly became tied to their real-life identities and were exploited for data manipulation and identification. The potential for targeting women, queer people, and other minorities that Lee Luda already had acquired from its real-time conversations got amplified as the bot could now also connect highly personal data to users, which could put them at risk of bodily harm. This database conflation and correlation in the name of interactivity eventually led to a fine of 103 million South Korean won for Scatter Lab (ibid., 19).

While the Lee Luda case might seem different from Facebook and Instagram cases, which often happen on the front end of the platform, it betrays a familiar pattern around data usage, consent, and circulation, which are often on the back end, extracted and mobilised by different AI intentions and machine-learning frameworks. Lee Luda finds similar parallels in big platforms offering multiple services in and outside the same geography, resulting in cross-contaminated data sets and leap-frogging consent that leads to extraction and transactability beyond the knowledge of the users affected. Interactivity, thus, is not just about users' interacting with each other or with digital assets but also about databases' connecting and interacting with each other, enabling the transactability of data.

Experts on law, policy, technology and society Chinmayi Arun and Smitha Krishna Prasad (2018) present a powerful reminder that transactability is a compromise of fundamental rights. Interactivity enables extraction and, hence, transaction of information and data structured around the spread of gendered violence and the exposure of vulnerable groups. Instead of the usual tropes of data ownership, transparency, consent, circulation, scope, and duration, which are the larger questions in the debate, we might need to take a pause and resist the idea of interactivity as a benign exercise of technological engagement.

If we position data as inalienable and treat data breaches and compromises through platformed breaches and circulation, we start realising that interactivity is a process of transactions that puts profits and circulation over safety and protection against harm. It is necessary to move away from the rhetoric of interactivity and identify it as a sinister attempt at making human data and its assemblages commodified and circulated in the platform economies. A gendered rewriting of the imperative of interactivity means identifying it as transactability, thus, immediately favouring data as live, embodied forms of being that are not to be compromised as negotiable elements of technological

design. In this rewriting, gender becomes an integral part of platformed data, as it is of our bodies, creating new structures of accountability that go beyond technological interventions.

Measures of Bodies

Scale is the promise of the network, interactivity the promise of the interfaces. The third promise of platforms is the production of measures. At the core of a digital platform is a set of standards, protocols, ontologies, and taxonomies that shape the ways in which information is measured. In one of the earliest theses on "The Language of New Media", Lev Manovich (2001) argues that the database – that spine around which platforms wrap – is a symbolic form and produces not only a description of the real but an alteration of it. Friedrich Kittler's milestone essay "There Is No Software" (2014) equally argues for recognising that the material infrastructure of governance and control are what defines platforms and the languages in which they are built. Kavita Philip, Lilly Irani, and Paul Dourish (2010) trace the postcolonial legacies of measurement and control that our modern-day computation devices carry. Maya Indira Ganesh (2017) argues that the measure, as in the case of the establishment of ethics in autonomous vehicles and AI, is a discursive production that is malleable and subject to constant revisions and fashions. Noopur Raval and Simiran Lalvani (2022) argue that platforms of the gig economy do not just formalise practices of life and labour but actually create new spaces for negotiations of global norms and their local operations.

Platforms measure things. They definitely measure gender, assigning different values, typologies, and worth to different gendered bodies and representations. However, the real promise is not about measuring as such; almost all media and technological forms measure in some way. Platforms, however, create measures to which the individual has to measure up. In our book "Really Fake", Alexandra Juhsaz and I (2021) argue that digital virility constantly demands that bodies and identities be technologically, socially, culturally, and politically persistent and consistent. The technological protocols that produce a continued performance of TCP/IP (Transmission Control Protocol/Internet Protocol) pings,[5] the networks that keep themselves alive through a steady shifting of data even in their state of redundancy, and the verification that happens through meta data

5 When looking at computational networks not just as carrying human authored information but shifting "machine traffic" – the different information that establishes connections, verification, and transfer of information between different digital devices in a network, we get to understand the larger contexts of information sharing that happens in this network. The protocols of TCP/IP, which allow for basic digital connections within a network also are the gateway for complex transfer of information which keep the system alive even when human triggered exchanges might not be happening.

production of traces and proof of work are all ways by which digital platforms are designed to engineer trust only towards technological nodes that can be consistent in their self-definition.

This technological demand for consistency in the nodes is what Alexander Galloway (2006) marks as a form of control through the production of protocols. It can also be traced back to William Gibson's first idea of cyberspace as a web made of "legitimate users" (1984) who can operate only when verified through the platform environments in which they are working. This idea of the verified and legitimised user came to the fore in the gamut of platforms and apps that were produced to manage the global COVID-19 pandemic.

With COVID-19, across the world, there was a concentration on technologies of trace, track, flag, signal, surveillance, and containment, all for managing public health. From the very early days of the lockdowns, we were downloading apps, showing certificates to scan at entrances, and consenting to have our phones tracked via Bluetooth. In many parts of the world, this (almost) ended in incarceration-like quarantine.

In India, the government introduced the platform Aarogya Setu, which tracked COVID-19 infections and monitored the movement of people marked as potentially infected. Legal scholar Smitha Prasad (2021) shows how Aarogya Setu was a combination of many different applications of contact tracing, quarantine, and crowd trackers, telemedicine providers, and simple public health information providers. She documents its evolution as it later also included registrations for vaccines and immunity passports.

While this seems like standard practice, one of the biggest features that makes Aarogya Setu interesting for the study of platform measures is its self-monitoring and policing function. Those detected as COVID-19-positive had to keep their phones online all the time – connected to the Internet and with Bluetooth enabled – so that it could be ensured that they were not leaving quarantine. This meant connecting the mobility of the device directly with the movement of the body. Additionally, patients in quarantine had to send selfies on a regular basis, several times a day, enabling geo location tags, to show and prove that they and their phones were in the designated spaces for quarantine (Datta 2020). This extraordinary combination of privacy invasion and surveillance was accepted as essential and was also opened up to private technology suppliers, service providers, and infrastructure intermediaries that could store and use this information for their own machine-learning health-monitoring experiments in e-health interventions and algorithmic modelling of contagion.

Aarogya Setu presented itself as a measure of the pandemic but was essentially a surveillance system for which users had to perform a consistent set of

performances and practices. Any deviation in the expected narratives – having to leave home for urgent reasons, low technological literacy preventing constant connectivity, lack of financial and digital resources for providing proof of containment – resulted in strict and harsh penalties and seclusions. It is important to note that unlike the larger, intentional harm coming from social media platforms as discussed at the beginning of this paper Aarogya Setu was not developed to target women. However, as Sheila Jasanoff and Sang-Hyun Kim (2015) point out in their framework of "sociotechnical imaginaries", these platforms are often skewed against women, who generally have lesser or minimised access to these digital devices. When digital platforms become the only measure, those bodies that are underprivileged via intersectional categories of class, religion, literacy, and caste immediately become unable to bear the burden of performing verification.

In the case of Aarogya Setu, not performing (or not being able to perform) verification had immediate dire consequences – the bodies of those unverified were marked as "deviant"; they became test cases and the subjects upon which conditions of punishment, surveillance, containment, and penalisation were modelled. The platform first produced measures that set many women up for failure because their daily rhythms and different levels of access to infrastructure had not been taken into account in the platform's modelling. Because the women did not correspond to these models, they were typified as potentially deviant and subjected to even more surveillance and control. In the process, data about their bodies and social contexts were extracted, and an entire data economy based on harvesting women's bodies and lives for data was built.

The promise of measures needs to be rewritten by the right to be forgotten. If it is impossible to build measure-free platforms, then the immediate mitigation for assuring gender-related safety and well-being must be to operationalise a self-erasing history of measurement in which measures and their values cannot be remembered, stored, archived, patterned or modelled beyond the immediate moment of measurement. The counter to platform measures is not countermeasures or transparency about the process of measurement and archiving but changing the very condition through which the results of measures are stored.

This is a conversation that has recently and suddenly started in the USA, where after the historic overturning of women's sexual and reproductive autonomy in the Roe v. Wade judgement by the Supreme Court, people suddenly realised that the quantified self apps on their phones might betray them and make them vulnerable (Perez 2022). While these apps are not directly connected to the government, there is palpable anxiety that state bodies might be able to demand access to app data, either for policing or for use as legal evidence

to persecute women who exercise their reproductive autonomy. For example, period-tracking or menstruation and ovulation femtech apps might recognise a delay or irregularity in menstrual health as potential proof of "deviance" from the law. These apps are not just measuring women's bodies but are actually measures themselves that detect any irregularity as deviance.

With this paper, it has been my intention to complicate the relationship between platforms – as symptomatic of the new artificial-intelligence-driven, data-anchored digital technologies with which we are living – and the ideas and imaginaries of gender and how the latter is studied in this interaction. By drawing together critical infrastructure studies, platform studies, digital cultures, and gender studies, my intention is to offer gender not as a site of inquiry but as a methodological tool when it comes to understanding the politics and accountability of digital platforms. I want to reiterate that while there is much work needed on thinking about platform and digital regulation to protect specific gendered bodies and people, there is still not enough attention being paid to how gender imaginaries and algorithmic practices of violence and extraction are not the afterthought of platform applications but lie at their very core. When thinking about digital gender, we can start thinking about gender not as something that is invoked in the application but already in the very construction of the platforms that we use and embody. This attempt at rewriting what I call platform promises by deploying gender as an analytic tool as well as a central organising principle of networked platforms is a way of approaching the problematic space of platformisation beyond just the revelatory mechanism of crisis and despair. Locating gender as endemic to understanding technological platforms allows us to think about new modes of negotiation and agency, vitalising the idea that platforms and gender are co-constitutive. Our role as researchers and practitioners is going to be to rewrite technological promises beyond just technological solutions.

References

Abidin, Crystal (2018): Internet Celebrity. Understanding Fame Online. Bingley: Emerald. doi: 10.1108/9781787560765

Association for Progressive Communications (2017): Online Gender-Based Violence. A Submission from the Association for Progressive Communication to the United Nations Special Rapporteur on Violence Against Women, its Causes and Consequences. https://www.apc.org/en/pubs/online-gender-based-violence-submission-association-progressive-communications-united-nations (07.10.2023).

Association for Progressive Communications (2016): Feminist Principles of the Internet. Version 2.0. https://www.apc.org/en/pubs/feminist-principles-internet-version-20 (07.10.2023).

Arkenbout, Chloë/Wilson, Jack/de Zeeuw, Daniel (Ed.) (2021): Critical Meme Reader. Global Mutations of the Viral Image. Amsterdam: Institute of Network Cultures. doi: 10.25969/mediarep/19281

Arun, Chinmayi/Prasad, Smitha Krishna (2018): Towards a Data Protection Framework. Social Science Research Network. doi: 10.2139/ssrn.3151222

Auslander, Philip (2012): Digital Liveness. A Historico-Philosophical Perspective. In: PAJ. A Journal of Performance and Art 34 (3), 3–11. doi: 10.1162/PAJJ_a_00106

Barabási, Albert-László (2002): Linked. The New Science of Networks. Cambridge: Perseus.

Benkler, Yochai (2006): The Wealth of Networks. How Social Production Transforms Markets and Freedom. New Haven: Yale University Press.

Chun, Wendy Hui Kyong (2021): Discriminating Data. Correlation, Neighbourhoods and the New Politics of Recognition. Cambridge: MIT Press. https://doi.org/10.7551/mitpress/14050.001.0001

Chun, Wendy Hui Kyong/Friedland, Sarah (2015): Habits of Leaking. Of Sluts and Networks Cards. Differences 26 (2), 1–28. doi: 10.1215/10407391-3145937

Datta, Ayona (2020): Self(ie)-Governance. Technologies of Intimate Surveillance in India under COVID-19. In: Dialogues in Human Geography 10 (2), 234–237. doi: 10.1177/204382062092979

Dibbell, Julian (1993): A Rape in Cyberspace: How an Evil Clown, a Haitian Trickster Spirit, Two Wizards, and a Cast of Dozens Turned a Database into a Society. http://www.juliandibbell.com/texts/bungle_vv.html (07.10.2023).

Dutta, Prabhash (2022): Who are Trads, the dangerous group Bulli Bai founder belongs to? https://www.indiatoday.in/india/story/trads-dangerous-group-bulli-bai-founder-sulli-deals-1898457-2022-01-11 (07.10.2023).

Galloway, Alexander R. (2006): Protocol. How Control Exists after Decentralization. Cambridge: MIT Press.

Ganesh, Maya Indira (2017): Entanglement. Machine Learning and Human Ethics in Driver-less Car Crashes. In: APRJA. A Peer-Reviewed Journal about Minor Tech 6 (1), 7–87. doi: 10.7146/aprja.v6i1.116013

Gibson, William (1984): Neuromancer. New York: Penguin Putnam.

Gillespie, Tarleton (2017): The Platform Metaphor, Revisited. In: Culture Digitally. https://www.hiig.de/en/the-platform-metaphor-revisited/ (07.10.2023).

Haugen, Frances (2021): Statement of Frances Haugen. Whistleblower Aid. Unites States Senate Committee on Commerce, Science and Transportation. https://www.commerce.senate.gov/services/files/FC8A558E-824E-4914-BEDB-3A7B1190BD49 (07.10.2023).

Helmond, Anne (2015): The Platformisation of the Web. Making Web Data Platform Ready. In: Social Media + Society 1 (2). doi: 10.1177/2056305115603080

Iyer, Neema/Nyamwire, Bonnita/Nabulega, Sandra (2020): Alternate Realities, Alternate Internets. African Feminist Research for A Feminist Internet. Pollicy. https://ogbv.pollicy.org/report.pdf (07.10.2023).

Jasanoff, Sheila/Kim, Sang-Hyun (Ed.) (2015): Dreamscapes of Modernity. Sociotechnical Imaginaries and the Fabrication of Power. Chicago: University of Chicago Press. doi: 10.7208/chicago/9780226276663.001.0001

Juhasz, Alexandra/Shah, Nishant (2021): Introduction. In: Juhasz, Alexandra/Langlois, Ganaele/Shah, Nishant (Ed.): Really Fake. In Search of Media. Minneapolis: University of Minnesota Press, Lüneburg: Meson Press, ix–xii.

Kayyali, Dia (2015): New Report Shows European Data Protection Authorities are Taking Facebook's Questionable Terms of Service Seriously'. https://www.eff.org/es/deeplinks/2015/02/new-report-shows-european-data-protection-authorities-are-taking-facebooks (07.10.2023).

Kim, Kelly (2020): Recent Debates on Data Utilisation and Protection. 3 Data Laws and Lee Luda. In: Shah, Nishant (Ed.): Platform Futures. Data Opportunities and Challenges. Hong Kong: Digital Asia Hub, 13–35. https://www.digitalasiahub.org/small-books-for-big-platforms.

Kittler, Friedrich A. (2014): The Truth of the Technological World. Essays on the Genealogy of Presence, 219–229. Translated by Erik Butler. Redwood City: Stanford University Press. doi: 10.1515/9780804792622-016

Losh, Elizabeth (2016): Hiding Inside the Magic Circle. Gamergate and the End of Safe Space. https://www.boundary2.org/2016/08/elizabeth-losh-hiding-inside-the-magic-circle-gamergate-and-the-end-of-safe-space (07.10.2023).

Malhotra, Namita (2015): Good Questions on Technology-Related Violence. https://www.apc.org/en/pubs/good-questions-technology-related-violence.

Manovich, Lev (2001): The Language of New Media. Cambridge: MIT Press.

O'Neil, Cathy (2016): Weapons of Math Destruction. How Big Data Increases Inequality and Threatens Democracy. New York: Crown.

Pandey, Geeta (2021): Sulli Deals. The Indian Muslim women 'up for sale' on an app. https://www.bbc.com/news/world-asia-india-57764271 (07.10.2023).

Perez, Sarah (2022): Consumers Swap Period Tracking Apps in Search of Increased Privacy Following Roe v. Wade Ruling'. https://techcrunch.com/2022/06/27/consumers-swap-period-tracking-apps-in-search-of-increased-privacy-following-roe-v-wade-ruling (07.10.2023).

Philip, Kavita/Irani, Lilly/Dourish, Paul (2010): Postcolonial Computing. A Tactical Survey. In: Science, Technology, & Human Values 37 (1), 3–29. doi: 10.1177/0162243910389594

Poell, Thomas/Nieborg, David/van Dijck, José (2019): Platformisation. In: Internet Policy Review 8 (4), 1–13. doi: 10.14763/2019.4.1425

Prasad, Smitha Krishna (2021): Covid-19 and Public Health Platforms in India. In: Shah, Nishant (Ed.): Platform Futures. Data Opportunities and Challenges. Hong Kong: Digital Asia Hub, 53–73. https://www.digitalasiahub.org/small-books-for-big-platforms.

Ramesh, Mythreyee (2021): 'Sulli Deals'. How Photos of Muslim Women were Misused on a GitHub App. https://www.thequint.com/neon/gender/sulli-deals-photos-of-muslim-women-misused-github (07.10.2023).

Raval, Noopur/Lalvani, Simiran (2022): The Moral Economy of Platform Work. In: Asiascape. Digital Asia 8 (1–2), 144–174. doi: 10.1163/22142312-bja10031

Salim, Mariya (2022): 'Bulli Bai', 'Sulli Deals': On being put up for 'Auction' as an Indian Muslim Woman. https://thewire.in/communalism/indian-muslim-woman-auction-bulli-bai (07.10.2023).

Scholz, Trebor (2016): Platform Cooperativism. Challenging the Corporate Sharing Economy. New York: Rosa Luxemburg Stiftung.

Shah, Nishant (2016): Exposing Pornography: The body between the old and the new. In: Chun, Wendy Hui Kyong/Fisher, Anna Watkins/Keenan, Thomas (Ed.): New Media, Old Media: A History and Theory Reader. New York: Routledge, 539–551.

Sinha, Jignasa/Siddigue, Iram (2022): Delhi Police Arrest BCA Graduate from Indore for Hate App Case Filed in July. https://indianexpress.com/article/cities/delhi/delhi-police-arrests-indore-man-sulli-deals-app-7714046 (07.10.2023).

Tsing, Anna Lowenhaupt (2012): On Nonscalability. The Living World is Not Amenable to Scales. In: Common Knowledge 18 (3), 505–524. doi: 10.1215/0961754X-1630424

Wang, Tricia (2013): Why Big Data Needs Thick Data. http://ethnographymatters.net/blog/2013/05/13/big-data-needs-thick-data (07.10.2023).

Zakaria, Rafia (2021): Against White Feminism: Notes on Disruption. New York: Norton & Company.