COMMENTARY

Data and privacy: Putting markets in (their) place

REETIKA KHERA

Abstract

Should privacy be a tradeable right? This is an issue for urgent consideration, given how much personal data collated from different sources can reveal about our personal lives. The rise of digital technologies and of the digital economy on the one hand, and of data mining capabilities on the other, present economic opportunities that are being harnessed, often at the cost of our privacy. Some see this as a case of "missing markets", where appropriate markets with adequate rules and regulations should be put in place. In this paper, I argue that the creating of a market for personal data, amounts to making the right to privacy a tradeable right. Further, a market for personal data/ privacy has all the characteristics of what Debra Satz characterises as "noxious markets". Other economists, notably Bowles, Hausman and MacPherson and Sandel, have sought to delineate the moral limits to markets in cases of child labour, the organ trade, etc. I argue that the market for personal data should be treated similarly.

Keywords: *privacy, personal data, limits to markets, ethics*

Introduction

In 2008, we met a National Rural Employment Guarantee Act (NREGA) worker in Sonebhadra district, Uttar Pradesh, who was owed nearly Rs 20,000 in NREGA wages, for work done over two years. A few months later, we learnt that his arrears were cleared. Out of curiosity we asked him what he did with the money, he told us that he had "invested" it. When we examined his papers, we realised that he had been duped of the entire amount. Information about his payment had been leaked to an unscrupulous operator. This was a salutary lesson on the importance of privacy of seemingly innocuous financial information, and the vulnerability of people to fraud when their personal (financial) data is compromised.

In 2017, a nine-judge Constitutional bench of the Supreme Court of India declared the right to privacy a fundamental right [1]. The case arose in the context of the Aadhaar (India's biometric/digital ID programme) matter and marked an important moment in the debate on privacy in the digital age. In the course of these hearings, there were attempts to trivialise privacy concerns by the government as well as by influential media voices [2]. Partly as a result of that judgment, debates in India today do not always need to start with a discussion on why the right to privacy is not an elitist concern, but of consequence to *everyone*. What is not as well understood is how our personal data can compromise our right to privacy.

The scope of our digital lives has expanded exponentially beyond economic activities (from prescriptions to food, work) to social media and personal activities (entertainment through OTT). What I eat, read, watch, who I meet or talk to, and how often, where, when and how I travel, and so on, is information readily available to others. Some products of companies such as Facebook and Google, pioneers in these intrusive technologies, could access private information [3,4]. Easier and cheaper storage implies more data can be stored for longer. Acquisti, Taylor and Wagman provide an overview of the thinking in economics on privacy and personal data, including the varied use of personal information by firms to influence consumer behaviour [5]. They suggest that privacy is a hard problem, that protection of privacy can "enhance and detract from individual and society welfare" and how consumers are at a particular disadvantage due to asymmetric and imperfect information.

This, in turn, has led to the use of our personal data to profile us, with the intention of predicting and even manipulating our behaviour [6]. The data broking industry is thriving and facilitates data mining [7]. Data analytics has proven profitable for businesses: for instance, in recent years, estimates suggest that around 80% of Google's total revenues come from advertising [8]. Much of this is driven by making our profiles — our searches (on Google and related products), characteristics (eg, our location and language), even our "personally identifiable information" (PII), data (address, date of birth, mobile phone numbers) — available to advertisers to help them target ads better [9].

One response to such worries is that we should treat this as a "missing market" [10] or incomplete markets problem. We need to put in place a regulatory framework, the argument goes, clearly specifying the rules for such transactions [11]. The authors state that "The ideal public policy setting is one in which individuals have property rights over personal information and can control and monetize their own data." Right now, individuals are not really reaping the fruits of being "data rich" because companies are able to mine their data without (adequately) compensating people. Thus arises an argument for creating "data rights" or "property rights" over data, that would allow people to monetise it, should they so wish [12].

For Matthan, a data rights-based approach will help overcome the limitations of the current consent-based model [13]. By allowing the rules of the game to be specified in law, we can "empower the individual" [14]. An extension of

this view is that privacy is a "luxury good" for which those who value it will have to pay a suitable price [15]. Incidentally, this view is diametrically opposite to the Supreme Court ruling in India declaring the right to privacy a fundamental right [1].

Besides the private sector, the government, too, is a vast repository of personal data — vehicle and property ownership, financial information, access to welfare, education, birth, death and health records, and much more. Though such data is held in a fiduciary capacity, it is also beginning to be seen as a business opportunity. For instance, "Over the last few years, the government and its agencies have acquired a goldmine of data with roll-out of initiatives like GST, Aadhaar, FASTag, e-bills, banking data with regulators, etc. Management and monetization of this large pool of data can be more effective and revenue-generating with private sector partnership with all relevant data protection covenants. Some of this data may already be getting used by the private sector for expanding their business and reach. An adequate framework on right mining and monetization of this can be invaluable for the government. Given the focus on digitization, the data can be used more productively and generate value for everyone." [16]

This view was exemplified in the *Economic Survey 2018-19* in a chapter titled "Data 'Of the People, By the People, For the People' " [17]. In 2019, the Indian government monetised motor vehicle registration data under the "Bulk Data Sharing" policy [18]. In response to privacy concerns from such sales, the data sharing policy was scrapped and no other incident has been reported since. Karnataka has already moved to put a "consent" framework (*e-Sahmati*) in place to allow private companies to access and verify education records with the state government, also held in a fiduciary capacity [19]. What one observes is a worrying marriage of convenience between "Big Data" and "Big Brother" [18, 20].

Some of this thinking was reflected in a draft of a Data Protection Bill proposed in 2018. That Bill and the Digital Personal Data Protection Act 2023 create a legal framework for facilitating the use of personal data for commercial purposes and protecting privacy when this happens. As the objectives of the 2023 Act put it: the law is intended to "provide for the processing of digital personal data in a manner that recognises both the right of individuals to protect their personal data and the need to process such personal data for lawful purposes". In the earlier Bill, the objective was worded slightly differently as being "necessary to create a collective culture that fosters a free and fair digital economy, respecting the informational privacy of individuals, and ensuring empowerment, progress and innovation through digital governance and inclusion…". "Lawful purpose" is defined in the law as "any purpose which is not expressly forbidden in the law" (Section 4(2)). Section 36 grants similar blanket permission to the government to "furnish such information as it may call for" from data fiduciaries, the Data Protection Board or others. I argue here that a framing where we are faced with a trade-off between the right to privacy and reaping the economic opportunities from digitalisation and data mining is problematic. We need to step back from the data rights line of thinking and critically view a market for personal data as one that makes the right to privacy a tradeable right.

Markets for personal data make privacy a tradeable right

In many situations, third party sale and/or mining of our personal data amounts to a violation of our privacy. However, even if individuals were to sell their own data, it would amount to surrendering their privacy. Narayanan and Schmatikov explain how our personal data and personally identifiable information are related to privacy violations [21]. Some examples help to think through some of these concerns. For instance, a food aggregator selling information about the frequency with which a customer orders food and the type of food ordered to a private health insurance company, that in turn, classifies this information as healthy vs greasy food to determine whether that customer gets medical insurance or not, would harm their interests.

"Flo", a period tracking app available globally, lied to its users about its privacy policy and shared information about menstruation dates and pregnancy plans with Facebook and Google [22]. Following the United States Supreme Court's decision that makes abortion illegal, there were worries about reproductive health apps becoming turncoats and handing over sensitive data to government agencies during criminal investigations [23, 24].

Similar worries arise in other contexts as well. Mental health apps are one such, where users share intimate information that can be stigmatising. Mozilla Foundation have flagged this issue: "The vast majority of mental health and prayer apps are exceptionally creepy. They track, share, and capitalize on users' most intimate personal thoughts and feelings, like moods, mental state and biometric data", cited in Goswami [25]. Further, the report says, "they routinely share data, allow weak passwords, target vulnerable users with personalized ads, and feature vague and poorly written privacy policies." Singh reports on a *Politico* investigation by Alexandra Levine where they found that a "Crisis Text Line" (CTL), a suicide helpline, shared data on conversations with people they had supported with their for-profit subsidiary to develop a related software [26]. CTL's defence was that data was anonymised. If the mental health apps have data broking subsidiaries with whom data is shared (as part of its privacy policy), the user of the app may end up getting de-anonymised and then being red flagged in all sorts of situations, eg, by a Curriculum Vitae (CV) sorting software to select job applicants.

When you order using an app or website for your first online order, you may be offered a first-use free coupon/ top-up. By downloading and using the app, you create a data footprint. In addition, you might be offered another reward worth, say, Rs 100 if you "refer a friend". This is a useful example to

distinguish between data footprints and "data shadows" [27] or "data externalities" [28]. Shadows refers to information about me on the internet, not because of my own activity, but through the activities of others — eg, when a person is trading someone else's data. Or, when I download a taxi hailing app, and it accesses contacts from my contact list and sends *them* notifications and promotions. Inadvertently, my digital footprint creates a data shadow of all my contacts, and compromises their privacy. Acemoglu provides a helpful overview of the harms that arise from such data practices [28]. For instance, platforms end up capturing most of the consumer surplus (the difference between what a consumer is notionally willing to pay and what they actually pay), with AI intensive firms benefitting more than others. Tirole also describes some of the analytical challenges for economists that arise with rapid digitisation [29].

Thus far, such private sector practices have hidden behind a facade of consent-based data mining (which implies that people have provided consent when they signed up for an app or used a website) and de-anonymisation of data (ie, that "personally identifiable information" is removed when data is sold), when it is sold. Personal data is being monetised supposedly with the individual's consent, whereas in fact, consent is only theoretical. A summary of a similar view advanced by economist Hal Varian (at Google) is available in Zuboff [30]. The limits of the consent-based market for data sharing, for example, people blindly accepting Terms and Conditions of privacy policies are now well understood. Privacy policies essentially ask for permission to access data on our devices. Another defence has been that data, when sold, are anonymised. This again, is an inadequate defence, as de-anonymisation has been shown to be easy to do [31]. A market for personal data, then, amounts to trading our privacy. Further, given that even governments succumb to the temptation to buy personal data for profiling, there is little hope of ethical practices surviving, even in businesses where they hope to do so [32].

Economics and the "limits of markets"

Should privacy be a tradeable right? Several economic philosophers have cautioned about the limits of markets. For instance, Hausman and MacPherson discuss the work of Richard Titmuss and Kenneth Arrow on blood donation [33, 34, 35]. Would blood donations be more efficient if they were commercialised, or voluntary? Both suggest that voluntary blood donations may be more efficient; because in a commercial system there can be an incentive for the donor to lie about whether their blood is safe. In addition, in certain situations, Titmuss felt a commercial system can discourage giving; since a potential blood donor may feel less moral compulsion to go out and donate if she knew that blood was available for a price [34].

Satz discusses "noxious markets" that are "toxic to important human values" [36]. Some markets shape our politics and culture and our identities, and may evoke discomfort, even revulsion. She argues that efficiency cannot be the only metric to evaluate markets. From markets for weapons and pollution on the one hand, to votes and mercenaries on the other, bans may be justified *even if* bans lead to inefficiencies. Further, there may be reasons to worry about certain markets even when egalitarian concerns are absent (say, that child labour is wrong even if it is not forced by destitution). Further, she endorses TH Marshall's view against markets for education, employment, healthcare and votes, because these are essential for a functioning democracy, and such goods should be guaranteed as rights. If markets undermine the equal status of people in what she calls the "social democratic" sense, ie, "… certain goods need to be provided outside the market if citizens are to be equals. Equality in these goods is necessary for democratic citizenship …", then such markets are questionable [36: p 208]. I believe that privacy (and therefore, personal data) should be treated in a similar way — as a social good and a right that is necessary for democratic citizenship.

Satz lists four parameters to gauge markets for noxiousness [36]. In the next section, I discuss to what extent personal data markets have these features:

1. *Vulnerability:* When people accept the terms of an exchange due to desperation (eg, the sale of child labour due to poverty).
2. *Weak agency:* When participants have poor information (information asymmetry), or in which they are not direct participants (eg, when elected leaders decide on behalf of voters).
3. *Extremely harmful outcomes for individuals:* When participation makes them destitute or harms their basic interests.
4. *Extremely harmful outcomes for society:* When they undermine an equal society or support relations of humiliating subordination or unaccountable power.

Sandel raises similar concerns [37]. Commodifying a good can alter its character. Market transactions in spheres of life that were governed by nonmarket transactions, crowd out the nonmarket moral and civic norms. Apart from a "fairness" argument, he makes a "corruption" argument, the degrading effect of such transactions (eg, if justice can be bought or sold), which applies even in the absence of inequality. I argue that personal data markets also create this sense of unease.

Characteristics of the personal data/ privacy market

Privacy falls in the same category of social goods/ rights as education, healthcare, justice, etc. In this section, I show that the market for data/ privacy has all the troubling characteristics discussed by Hausman and McPherson, Satz and Sandel [33, 36, 37]. In particular, it satisfies the test for a "noxious market" described by Satz, summarised above.

Efficiency

One argument for sharing personal data is that they can enhance "efficiency" in our online lives. However, that is not always the case. Often, the argument in favour of such markets highlights the monetary value of small bits of data and how we all benefit, say, personalised and auto-suggestions while shopping online can reduce search time if information on our preferences is made available through sharing personal data. This seemingly "win-win" situation (sellers gain buyers and buyers' search costs are reduced) in fact hides an inherent asymmetry. The same data mining algorithms that can target ads also enable companies to extract all consumer surplus and to manipulate consumers. Cathy O'Neil gives the example of how algorithms suss out our vulnerabilities to exploit them. For instance, when a person goes looking for shoes online, the algorithm may suggest socks or other complementary goods [38]. If you want to educate yourself about "how to invest", you may be targeted with ads for investing options.

Some products that are purportedly created to enhance consumer utility, like suggestions and targeted advertising on Netflix, Amazon, YouTube, etc, are, in fact, designed to promote addictive behaviour. Are such practices morally acceptable? One could argue, for instance, that the algorithms help save search time and that people who browse are doing so of their own choice. On the other hand, promotion of other addictive products (eg, alcohol, tobacco products, etc) is restricted precisely on the grounds that it undermines a person's ability to make a choice. Moreover, there is a question about how prices for our personal data are to be determined in such markets.

Vulnerability/egalitarian concerns

One illustration of unfair, or at least, questionable practices is that of Byju's, an online tutoring firm, and the world's highest-valued edtech start-up at one time. During the school closures due to Covid in 2020-21, Byju's pushy and aggressive agents and managers preyed on parents' anxieties about school closures and their child's future. Byju's offered a free download for the first 15 days, monitored usage in that period, and those who used the app frequently were called by Byju's agents. Children were asked questions that the agents knew the kids were likely to fail, heightening the anxiety parents felt for their child's future, got them to sign up, offered loans with hidden terms and conditions, only to disappear or under-deliver subsequently [39, 40].

There are similar reports of people entitled to welfare benefits (wages under the National Rural Employment Guarantee Act 2005, social security pensions, maternity benefits and so on) who were forced to first get Aadhaar, then sign a "consent" on data sharing. The "option" they had was to walk away from these welfare benefits or consent to data sharing — the consequences of which they did not understand.

Weak agency due to information asymmetry and lack of meaningful consent

In case of morally acceptable data trades, how does one determine whether people are getting a fair compensation? After all, the company is likely to benefit from a stream of purchases from the person you refer. When someone shares her data because a Rs 100 coupon is of some consequence to her (eg, students recommending friends), both parties are better off, the user has been compensated for sharing her data; yet Satz' and Sandel's fairness argument is very much at play. The app developers are targeting a market segment, eg students, that is willing to share data at an undervalued price because that segment is likely to be cash–strapped. In this example, a friend who receives a Rs 100 coupon may not have got the true value of the information she shares (phone numbers from her contacts list). Further, she may not have comprehended what she has consented to: whether the app will share such information to monetise it further, or whether the app will share information with other apps that this is a customer who is willing to sell information for a Rs 100 coupon. According to one website, one sign up for an SMS service is worth USD 8 to a firm (see: https://tasil.com/data-value-estimator/).

More importantly, if she were fully aware of the uses to which such data are being put, would she still have shared the information? Data mining is used to extract consumer surplus (eg, the allegation that Uber used surge pricing when mobile battery charge was low [41]), to nudge us to buy more ("frequently bought with this product" suggestions), to put us in silos (based on what we read and who we follow), polarises society [42] and manipulates our economic and political decisions [43]. When customers download/ sign up for apps, are they aware of the wide-ranging consequences?

Incidentally, increasingly in online markets, sale/purchase is only possible if you part with your data (basic personal information) in a way that consumers are denied choice and freedom (for instance, the food aggregator Zomato only allows orders if their app is downloaded, not through the web). The lack of meaningful and informed consent is another aspect of the vulnerability in such markets.

Weak agency where digital shadows are involved

If a friend refers me, she creates a data shadow about my personal information (name and mobile number); while my own consent is bypassed (a routine occurrence). This is another aspect of the weak agency problem in the data market.

Extremely harmful outcomes for individuals

When we use mobile payment apps for digital transactions, we are putting some information about our financial transactions in the hands of the apps we use. Are people

really aware of whether information about those transactions is protected or shared further by the payment app? If all these transactions are routed through one server (National Automated Clearing House/National Payments Corporation of India), are they aggregating these data about us? If so, are they allowed to share this with anyone? Also, with whom and under what conditions?

What sorts of identity fraud do data mining opportunities open up, to the detriment of the consumer? Data breaches have jeopardised people's economic and personal lives. Phishing scams are often the result of such loss of control over one's data (eg, I share some personal information with a platform for verification and that is later shared with a third party)[1], and often the loss of control is executed surreptitiously. In India, reported cybercrimes especially those related to identity theft, online fraud (credit and debit cards, online banking, etc.) have increased more than five times, from just under 10,000 in 2014 to almost 53,000 cases in 2021, according to the National Crime Records Bureau [44, 45].

Extremely harmful outcomes for society due to negative externalities

The fact that data trades are essentially creating a market for privacy, and that the right to privacy is important for human growth, is the main reason that personal data markets are contentious. One could also characterise a compromised right to privacy as the negative externality associated with, or a toxic by-product of, data markets. Another harm would be to public discussion and democracy, when practices of social media platforms lead to polarisation. The testimony by Frances Haugen on how Facebook amplifies and monetises hate speech, and the effects of this on society is a recent example of this [46]. The practices of Cambridge Analytica in terms of profiling voters with a view to influencing outcomes on the basis of such analysis undermines democratic practice.

Degradation of social norms

Some social norms are endangered by our digital lives. I have in mind the degrading of personal relationships (birthdays, friendships, holidays are played out on social media), the phenomenon of "viral videos" that make lynchings and accidents a spectacle to capture on camera. Recently, in India, an app prompted users to "find your sulli deal of the day". (*"Sulli"* is a derogatory term for Muslims). The app used photographs of Muslim women, harvested from the internet (without their consent or even knowledge), and offered them to users. The app is both Islamophobic and misogynistic.

Remedies: Regulate, redistribute, restrain?

What do we do if a market is potentially noxious? Economists have proposed various remedies for dealing with market failures (such as the ones seen in the data market). However, Satz argues that certain market failures "shape our relationships with others in ways that goes [sic] beyond the idea of unabsorbed economic costs" [36: p 93]. These failures affect our standing before, during, and after the exchange.

Satz suggests a differentiated response depending on context, ranging from creating an alternative distribution mechanism alongside the market, redistribution, regulation and restraining such markets. Bowles warns that "fines, rewards and other material incentives often do not work very well" [47]. In a famous experiment by Gneezy and Rustichini, introduction of a fine for parents who did not punctually pick up their children from a day care centre, *increased* the number of such parents; the number did not go down even after the fine was removed [48].

Two prominent options for data/ privacy markets have been regulation and better control over data through creation of "data rights". The General Data Protection Regulation (GDPR) was guided by the EU charter which guarantees the right to privacy and data protection, and has been held up as a fine example. Yet, as I suggest below, this route has not been particularly effective.

Further, it has become accepted practice that apps are uploaded directly to mobile phone platforms offered by Apple and Google. While Apple has human review before approval is granted, in the case of Google, human review is only undertaken in case of complaints. Academy of Medical Sciences provides a helpful illustration of the challenges of regulating apps [49]. Developers of apps are not required to get any government clearance. This has created a free-for-all situation and given the scope of the "services" provided through apps (health advice, loans, payments, education, etc); this is an alarming situation. Yet one hears very little about bringing in government oversight or accreditation before apps are uploaded. Only in 2021, the Reserve Bank of India ordered Google to remove 30 loan apps [50]. RBI's actions were triggered by reports of intimidation, cyber bullying and even suicides on account of defaults by borrowers. According to news reports, some loan apps require the user to give access to their phone gallery, and later photographs taken from the gallery are used to bully borrowers [51].

In fact, in the Indian case, given that the debate was steered *away* from the right to privacy and data protection, *towards* the creation of suitable regulation for exploitation of this economic opportunity, legal safeguards are even less likely to work. This is evident from the *Economic Survey 2019,* the 2019 draft Bill on data protection, and government committees including the Srikrishna Committee and the joint Parliamentary committee [52]. For instance, the Srikrishna Committee report was titled *A Free and Fair Digital Economy — Protecting Privacy, Empowering Citizens*[2]. In its opening paragraph, the notification of the constitution of the committee states, "The need to ensure growth of the digital economy while keeping personal data of citizens secure and protected is of utmost importance."

When they work, markets regulation strategies can undermine markets

Bowles argued that incentives (or fines) alone cannot

provide good governance [47]. One can see a glimpse of that in a widely reported case, where French authorities imposed a fine of USD 57mn on Google for violating GDPR norms on transparency [53]. This seemingly large fine was in fact less than 0.1% of Google's annual turnover (USD 161 billion) and profit (USD 90 billion) in 2019. The GDPR, among the strongest data protection laws right now, allows a fine of up to 4% of the annual global turnover. But such cases are rare, and corporations are more likely to treat fines as operational costs, rather than as warnings to alter their practices substantively.

Market regulation strategies are a smokescreen

Zuboff (2019) warns that individuals "wrestling with the myriad complexities of their own data protection will be no match for surveillance capitalism's staggering asymmetries of power and knowledge" [30: p 482]. Can we truly expect that data markets will develop into ideal-type perfectly competitive markets, and that when people are allowed to trade their data if they like, that they themselves will be the beneficiaries? In a society with low literacy among certain segments, poor financial and digital literacy, can we be so naïve? In fact, even those with digital and financial literacy, easily and regularly fall prey to these techniques.

Another weakness in the argument that proposes the creation of a regulatory framework with penalties for violations is that the field is not balanced. It pitches poorly empowered citizens against powerful and invisible entities. If I am fortunate enough to understand how a data fraud was inflicted on me, and I seek redressal, it is not evident (as Zuboff anticipates) that pinning responsibility on the private entity is going to be possible, easy or costless to me. Individual or collective attempts to hold big corporations to account have been rare.

Conclusion

Like Zuboff, Milanovic argues that while globalisation and technological revolutions have created markets for new things (personal data, rentals for own cars and homes, etc), the commodification of ever-increasing spheres of human life — politics, leisure, data — is likely to lead to a crisis, if its "field of action" is not controlled and reduced to more traditional areas [54]. For Satz, "some markets are noxious and need to be blocked or severely constrained if the parties are to be equals in a particular sense, as citizens in a democracy" [36].

A reader might ask, where does this leave us? Perhaps greater digital literacy, privacy-respecting software, open standards, can make a difference. One way to move ahead is to ask whether tweaks in the data protection framework can show the way forward. Can the principles (purpose limitation, data minimisation, etc), grounds (consent, medical emergency, legal obligation), and rights (access, correction, erasure etc) provide remedies such that our equal standing (as Satz puts it) in such transactions is either promoted, or at least not undermined?

To suggest that such markets should be controlled, reduced or blocked is seen as impractical and idealistic. Yet, as Zuboff says, "the message of inevitability [that] is power's velvet-gloved right hand" must be rejected [30: p 522]. She ends her account of surveillance capitalism with a call to action, to "be the friction" and invokes Orwell who likens "the instinct to bow down before the conqueror of the moment" to a bad habit and a mental disease [30: p.523]. In *The age of surveillance capitalism,* Zuboff is open-minded about the effects of regulations such as GDPR, and stops short of suggesting a ban.

In India, we have allowed the debate on data markets and data protection to be framed in a way that accords primacy to harnessing the economic opportunities arising from data mining, or puts these opportunities on an equal footing with the right to privacy. This comes out clearly in the objectives of the DPDP Act 2023, as stated above. Perhaps this was because the link between data markets, data mining and the right to privacy was not apparent at the beginning. Perhaps this was because the scope of data mining has expanded beyond what one could have imagined. Or perhaps this is because it serves the interests of the powerful public and private entities, who in turn control the narratives. It is time to re-examine these issues by putting markets in their place: placing democracy and human rights above markets.

Note:

[1]*Say, my data (mobile number) is shared with an online platform for verification of a purchase on that platform. The platform is allowed to trade it further. A few such trades later, it falls into the hands of phishing scamsters, who are also buying similar personal data (eg, birth date, mother's maiden surname, etc) from other sources or advertisers of various goods (property deals, weight loss programmes, medical tests).*

[2]*https://www.thequint.com/news/india/key-highlights-from-srikrishna-committee-report-on-data-protection#read-more*

Author: Reetika Khera (reetika@hss.iitd.ac.in, https://orcid.org/0000-0001-9955-8087), Professor of Economics, Indian Institute of Technology Delhi, MS603 Department of Humanities and Social Sciences, New Delhi, INDIA

Conflict of Interest: None declared **Funding:** None

Acknowledgments: The author thanks Kritika Bhardwaj, Arudra Burra, Jean Drèze, Rajesh Jha, Anja Kovacs and G. Sampath for helpful discussions and comments.

To cite: Khera R. Data and privacy: Putting markets in (their) place. *Indian J Med Ethics.* 2026 Oct-Dec; 11(4) NS: 281-288. DOI: 10.20529/IJME.2026.014

Submission received: April 18, 2025

Submission accepted: February 11, 2026

Published online first: March 07, 2026

Manuscript Editor: Sunita Sheel Bandewar

Peer Reviewer: Akshay S Dinesh

Copyright and license

©*Indian Journal of Medical Ethics* 2026: Open Access and Distributed under the Creative Commons license (CC BY-NC-ND 4.0), which permits only non-commercial and non-modified sharing in any medium, provided the original author(s) and source are credited.

References

1. Supreme Court of India. *Justice K.S. Puttaswamy (Retd) vs Union of India on 26 September, 2018.* Wrt Petn (Civil) No. 494 of 2012 [Cited 2025 Dec 24]. Available from: https://indiankanoon.org/doc/127517806
2. Khera R. The different ways in which Aadhaar infringes on privacy.

The Wire. 2017 Jul 19 [cited 2025 Nov 25]. Available from: https://thewire.in/159092/privacy-aadhaar-supreme-court/
3. Briceno M. Are tech companies using your private data to train AI models. *Al Jazeera*. 2025 Nov 24 [cited 2025 Dec 20]. Available from: https://www.aljazeera.com/news/2025/11/24/are-tech-companies-using-your-private-data-to-train-ai-models
4. Federal Trade Commission. FTC approves final settlement with Facebook. 2012 Aug [cited 2025 Dec 15]. Available from: https://www.ftc.gov/news-events/news/press-releases/2012/08/ftc-approves-final-settlement-facebook
5. Acquisti A, Taylor C, Wagman L. The economics of privacy. *J Econ Lit*. 2016;54(2):442 92. http://dx.doi.org/10.1257/jel.54.2.442
6. Beauvisage T, Mellet K. Datassets: assetizing and marketizing personal data. In: Birch K, Muniesa G, editors. *Assetization: Turning things into assets in technoscientific capitalism*. Cambridge (MA): MIT Press; 2020[cited 2025 Dec 15]. Available from: https://www.researchgate.net/publication/335748286_Datassets_Assetizing_and_Marketizing_Personal_Data
7. Manikandan A, Palepu A. The great Indian data bazaar. *The Morning Context*. 2022 May 2[cited 2025 Dec 15]. Available from: https://themorningcontext.com/internet/the-great-indian-database-bazaar
8. Graham M, Elias J. How Google's $150 billion advertising business works. *CNBC*. 2021 May 18[cited 2025 Dec 15]. Available from: https://www.cnbc.com/2021/05/18/how-does-google-make-money-advertising-business-breakdown-.html
9. Cyphers B. Google says it doesn't "sell" your data: here's how the company shares, monetizes, and exploits it. *Electronic Frontier Foundation*. 2020 Mar [cited 2025 Dec 15]. Available from: https://www.eff.org/deeplinks/2020/03/google-says-it-doesnt-sell-your-data-heres-how-company-shares-monetizes-and
10. Ibarra IA, Goff L, Hernandez J, Lanier J, Weyl E. Should we treat data as labour? Let's open up the discussion. *Brookings Institute*. 2018 Feb 21[cited 2025 Dec 15]. Available from: https://www.brookings.edu/blog/techtank/2018/02/21/should-we-treat-data-as-labor-lets-open-up-the-discussion/
11. Berg C, Davidson S. Selling your data without selling your soul. Washington, DC: Competitive Enterprise Institute; 2019 Oct 7[cited 2025 Dec 15]. Available from: https://cei.org/studies/selling-your-data-without-selling-your-soul/
12. Rose E. Balancing Internet market needs with consumer concerns: a property rights framework. *Computers and Society*. 2001 Mar 1; 31(1): 6-11. https://doi.org/10.1145/572230.572233
13. Founding Fuel. The future of privacy. A conversation with Rahul Matthan. *Founding Fuel*. 2017 Sep 17 [cited 2025 Dec 15]. Available from: https://www.foundingfuel.com/article/the-future-of-privacy-a-conversation-with-rahul-matthan/
14. Nilekani N. Why India needs to be a data democracy. *Livemint*. 2017 Jul 27 [cited 2025 Dec 15]. Available from: https://www.livemint.com/Opinion/gm1MNTytiT3zRqxt1dXbhK/Why-India-needs-to-be-a-data-democracy.html
15. Szulik K, Maslin J. Is privacy a luxury good? *UC Berkeley School of Information Blog*. 2020 Feb 10 [cited 2025 Dec 15]. Available from: https://blogs.ischool.berkeley.edu/w231/2020/02/10/is-privacy-a-luxury-good/
16. Sanghai S. How privatization and data monetisation can solve India's fiscal deficit problem. *The Economic Times*. 2020 Oct 18[cited 2025 Dec 15]. Available from: https://economictimes.indiatimes.com/markets/stocks/news/how-privatization-and-data-monetization-can-solve-indias-fiscal-deficit-problem/articleshow/78731109.cms
17. Ministry of Finance, Government of India. *Economic Survey 2018–19*. New Delhi: Ministry of Finance; 2019 Jul [cited 2025 Dec 26]. Available from:https://www.indiabudget.gov.in/budget2019-20 economicsurvey/doc/echapter.pdf
18. Khera R. The makings of a digital kleptocracy. *The Hindu*. 2019 Jul 31[cited 2025 Dec 15]. Available from: https://www.thehindu.com/opinion/op-ed/the-makings-of-a-digital-kleptocracy/article28762504.ece
19. Jain A. Karnataka unveils its consent-manager framework for data sharing by citizens. *Medianama*. 2021 Dec 21[cited 2025 Dec 15]. Available from: https://www.medianama.com/2021/12/223-karnataka-consent-manager-e-sahmati-unveiled/
20. Khera R. Tale of two whistle-blowers. *Indian Express*. 2018[cited 2025 Dec 16]. Available from: https://indianexpress.com/article/opinion/columns/facebook-cambridge-analytica-artificial-intelligence-tale-of-two-whistle-blowers-5154413/
21. Narayanan A, Schmatikov V. Privacy and security: myths and fallacies of "personally identifiable information". *Commun ACM*. 2010;53(6): 24-26. https://doi.org/10.1145/1743546.1743558
22. Schiffer Z. Period-tracking app settles charges it lied to users about privacy. *The Verge*. 2021 Jan 14[cited 2025 Dec 16]. Available from: https://www.theverge.com/2021/1/13/22229303/flo-period-tracking-app-privacy-health-data-facebook-google
23. Moscufo M, Parks M, Taudte W. Period-tracking apps may help prosecute users, advocates fear. *ABC News*. 2022 Jul 2[Cited 2025 Dec 15]. Available from: https://abcnews.go.com/Health/abortion-advocates-fear-period-tracking-apps-prosecute-abortion/story?id=85925714
24. Garamvolgyi F. Why US women are deleting their period tracking apps. *The Guardian*. 2022 Jun 28[Cited 2025 Dec 15]. Available from: https://www.theguardian.com/world/2022/jun/28/why-us-woman-are-deleting-their-period-tracking-apps
25. Goswami T. Data. Ta-da! *Sanity by Tanmoy*. 2022 Jun 10[cited 2025 Dec 16]. Available from: https://www.sanitybytanmoy.com/mental-health-apps-data-privacy/
26. Singh D. Data v humans: this is how we win the battle for the future of mental healthcare. *Sanity by Tanmoy*. 2022 Mar 22[cited 2025 Dec 15]. Available from: https://www.sanitybytanmoy.com/data-v-humans-how-to-win-the-battle-for-the-future-of-mental-healthcare/
27. Kitchin R. *The data revolution: big data, open data, data infrastructures and their consequences*. London: Sage; 2014.
28. Acemoglu D. Harms of AI. *NBER Working Paper* No. 29247; 2021 Sep. https://doi.org/10.3386/w29247
29. Tirole J. *Economics for the common good*. Princeton (NJ): Princeton University Press; 2017. (Translated by Randall S.)
30. Zuboff S. *The age of surveillance capitalism: the fight for a human future at the new frontier of power*. London: Profile Books; 2019.
31. Narayanan A, Huey J, Felten E. A precautionary approach to big data privacy. 2016. In: Gutwirth, S., Leenes, R., De Hert, P. (eds) Data Protection on the Move. Law, Governance and Technology Series, vol 24. Springer, Dordrecht. Available from: https://doi.org/10.1007/978-94-017-7376-8_13
32. Ayoub E, Goitein E. Closing the data broker loophole. *Brennan Center*. 2024 Feb 13[cited 2025 Dec 15]. Available from: https://www.brennancenter.org/our-work/research-reports/closing-data-broker-loophole
33. Hausman D, McPherson M. Taking ethics seriously: economics and contemporary moral philosophy. *J Econ Perspect*. 1993 Jun;31(2): 671-731. Available from: https://www.jstor.org/stable/2728513
34. Titmuss R. *The Gift Relationship: From Human Blood to Social Policy*. Online edition. Bristol; Policy Press Scholarship Online. 2019 May 23 https://doi.org/10.1332/policypress/9781447349570.001.0001
35. Arrow G. Gifts and exchanges. *Philos Public Aff*. 1972;1(4):343 62. Available from: https://www.jstor.org/stable/2265097
36. Satz D. *Why some things should not be for sale: the moral limits of markets*. Oxford: Oxford University Press; 2010 May 12[cited 2025 Dec 16] https://doi.org/10.1093/acprof:oso/9780195311594.001.0001
37. Sandel M. *What money can't buy: the moral limits of markets*. Macmillan; 2013 Apr 2.
38. O'Neil C. *Weapons of math destruction: how big data increases inequality and threatens democracy*. Broadway Books; 2016.
39. Saha P. How Byju's catches parents. *The Morning Context*. 2020 Mar 11[cited 2025 Dec 15]. Available from: https://themorningcontext.com/chaos/how-byjus-catches-parents
40. Inamdar N. Byju's and the other side of an edtech giant's dizzying rise. *BBC*. 2021 Dec 7[cited 2025 Dec 15]. Available from: https://www.bbc.com/news/world-asia-india-58951449
41. Chowdhry A. Users are more likely to pay surge pricing if their phone battery is low. *Forbes*. 2016 May 25[cited 2025 Dec 15]. Available from: https://www.forbes.com/sites/amitchowdhry/2016/05/25/uber-low-battery/
42. Marcetic B. Facebook whistleblower and the case for public utility regulation. *Jacobin*. 2021 Oct[cited 2025 Dec 15]. Available from: https://jacobinmag.com/2021/10/facebook-whistleblower-haugen-profits-addiction-public-utility-regulation-censorship-moderation-zuckerberg
43. Corbyn Z. Facebook experiment found to boost US voter turnout. *Scientific American*. 2012 Sep 12[cited 2025 Dec 15]. Available from: https://www.scientificamerican.com/article/facebook-experiment-found-to-boost-us-voter-turnout/
44. Government of India. Crime In India. Statistics. Volume II. National Crime Records Bureau. Ministry of Home Affairs. 2014. Table 9A2, p. 752
45. Government of India. Crime In India. Statistics. Volume II. National Crime Records Bureau. Ministry of Home Affairs. 2021. Table 9A2, p.

786.
46. Statement of Frances Haugen before the US Sub-Committee on Consumer Protection, Product Safety, and Data Security, on October 4, 2021 [cited 2025 Dec 24]. Available from: https://www.commerce.senate.gov/services/files/FC8A558E-824E-4914-BEDB-3A7B1190BD49
47. Bowles S. *The moral economy: why good incentives are no substitute for good citizens.* New Haven: Yale University Press; 2016.
48. Gneezy U, Rustichini A. A fine is a price. *J Legal Stud.* 2000 Jan;29(1): 1-17. https://doi.org/10.1086/468061
49. Academy of Medical Sciences. Health apps: regulation and quality control. 2015. [cited 2025 Dec 17]. Available online: https://acmedsci.ac.uk/policy/policy-projects/health-apps-regulation-and-quality-control
50. Manikandan A, Shukla S. Google removes 30 loan apps from Play Store after RBI red flag. *The Economic Times.* 2021 Jan 15[cited 2025 Dec 15]. Available from: https://economictimes.indiatimes.com/tech/technology/google-removes-personal-loan-apps-violating-user-safety-policies-from-play-store/articleshow/80267043.cms
51. Dominic B. Puducherry crime branch gets 55 unauthorized loan apps removed. *Times of India.* 2022 Oct 1[cited 2025 Dec 15]. Available from: https://timesofindia.indiatimes.com/city/puducherry/puducherry-cybercrime-cell-gets-55-unauthorised-loan-apps-removed/articleshow/94580489.cms
52. Committee of Experts chaired by Justice B.N. Srikrishna. *A free and fair digital economy: protecting privacy, empowering citizens.* BN Srikrishna. 2018 Jul 27[cited 2025 Dec 15]. Available from: https://www.naavi.org/uploads_wp/new/Data_Protection_Committee_Report.pdf
53. Porter J. Google fined €50 million under GDPR. *The Verge.* 2019 Jan 21[cited 2025 Dec 15]. Available from: https://www.theverge.com/2019/1/21/18191591/google-gdpr-fine-50-million-euros-data-consent-cnil
54. Milanovic B. Why it is not the crisis of capitalism. 2019 Oct 16[cited 2025 Dec 15]. Available from: https://www.globalpolicyjournal.com/blog/16/10/2019/why-it-not-crisis-capitalism

COMMENTARY

Responsible Health-AI: Complex scenarios from a humanities perspective

SIBY K GEORGE

Abstract

The mega-cultural age of artificial intelligence (AI) is theorised in this paper referring to the Heideggerian phenomenology of technology and cybernetics. Arguing that resisting the logic of its age is beyond a subfield of ethics, the paper draws attention to the way medical ethics can reassess from within the framework of the age the new ethical dilemmas and complex scenarios brought about by health-AI. Two moral situations are discussed in this context: using Electronic Health Records for non-health-related purposes such as solving mystery crimes and using health-AI for new drug development and improved treatment protocols. The purpose of the discussion is to reexamine medical ethics in the age of AI without overlooking the complexities health-AI can engender.

Keywords: *Health-AI, ethical dilemma, EHR, drug development, Heidegger, cybernetics*

From all accounts available so far, the age of artificial intelligence (AI) appears to be a planetary epoch of mega-cultural transformation that affects all aspects of human existence and people everywhere. Because of their ubiquitous character, such epochal changes are neither good nor evil. In fact, they redefine good and evil, destabilise prevalent practices, and open up unforeseen possibilities. Owing to this, these changes generate previously unexperienced dilemmas and ambivalences. When a physician makes an error of judgement, it is clear who is responsible. But when a physician uses an AI-aid that makes an error, it is difficult to decide who is responsible — whether it is the physician, the developer of the AI-aid, or the institution that purchased it. This paper discusses the complex scenarios and ethical dilemmas arising from the age of AI — health-AI, to be precise. But the aim of the paper is not to idly generate new medical ethics riddles but to ponder over our new reality. This aim is non-normative for sure, but for that reason it is not unrelated to normative ethics. My concerns will be to show how complex, dilemmatic, and intractable the new moral scenario is in healthcare practice and how our present moral imagination and conceptual apparatuses are insufficient to deal with them. One of the important tasks of medical humanities, a phenomenological task if you will, is (as I see it) not to prescribe norms, but to shed light on the medical situation as it is experienced by the careful onlooker, away from its maddening urgencies without sacrificing its complexity and radical newness.

This paper will first develop a Heideggerian philosophical perspective on mega-cultural technological transformations — in this instance the revolutionising changes wrought by health-AI. Martin Heidegger, a twentieth-century German phenomenologist, is a pivotal thinker of the technological age, whose musings on the inchoate early stage of the cyber age are well-known. After developing this framing perspective in the first section, I will dwell briefly in the second section on the dilemmas and anticipations of the age of Health-AI. I will then discuss two scenarios of ethical dilemmas in medical situations. Section two will be on dilemmatic aspects of using Electronic Health Records (I) of private individuals (subjects of medical research or treatment or both) for non-health-related purposes. Section three will be on dilemmas in the use of AI for the discovery and development of new drugs and improved treatment. I will conclude with a few remarks on ethical dilemmas.

The mega-cultural epoch of AI

Human technological capability (as rudimentary tool-making) is generally believed to have predated human