# EXAMINING THE LEGAL FRAMEWORK GOVERNING DATA PROTECTION FOR FITNESS TRACKING WEARABLE DEVICES IN INDIA

*Rahul Krishna

**ABSTRACT**

*Health wearables have become increasingly pervasive and have access to vast amounts of private data of users. The objective of this article is to assess the state of legislation and regulation to ensure data protection in the case of health wearables in India. It attempts to highlight the existing protections afforded to citizens and the gaps that remain.*

*The study uses Healey's definition of "consumer products for health monitoring" as the set of devices examined.[1] These devices are collecting extensive health-related data from users using wearables. The paper subsequently contextualizes the challenges to existing concepts of privacy protection that internet-of-things devices present with health data monitored by fitness trackers. It examines the shortcomings of existing models of data protection for the scale and specificity of data captured by such devices.*

*The Government has proposed the Personal Data Protection Bill and the Draft Digital Information Security in Healthcare Act (DISHA) in addition to existing legislation governing health related data. The study assesses the protections extended by these regulations to health data collected by fitness trackers. It analyses the conceptual approach to data protection taken by these legislations and how it has been implemented in the document. The definitions also help identify the differences in approach and areas that need to be reconciled to ensure effective protection to data owners. The paper examines the existing set of protections afforded by law to such data as a contrast to the changes proposed, wrapping up with analysis of case law taking the judiciary's thought on the privacy requirements of health data.*

## I. INTRODUCTION

The recent past has seen rapid expansion in the uses and adoption of wearable technology commercially available. The technology itself has grown with advances in miniaturization to become a part of everyday life for many. These advancements have made devices like fitness trackers commercially viable. The industry for fitness trackers has witnessed unprecedented growth, reflected in Google's valuation of fitness tracker

* Rahul Krishna, Research Assistant, Observer Research Foundation

[1] Jason Healey, Neal Pollard, and Beau Woods, *The Healthcare Internet of Things: Rewards and Risks,* Atlantic Council, available at https://www.atlanticcouncil.org/wp-6content/uploads/2015/03/ACUS_Intel_MedicalDevices.pdf, last seen on 14/12/2019.

manufacturer Fitbit at $2.1 Billion.[2] India has adopted such products rapidly as well, becoming the 3rd largest market for wearable devices in the world in 2019.[3] Studies estimate that 2019 saw the sale of a 100 million units of such devices all across the world and the number is expected to grow.[4] Research also shows that adoption in countries such as the US shows that one in five adults use fitness trackers, with the number being even greater for higher income groups.[5]

However, these devices also pose significant privacy risks for individuals with the nature of data being collected by them. Data collected by such wearable devices is some of the most intimate data for humans. Such data is highly valued by several industries and it is crucial to establish a robust framework for protecting such data. The privacy risks posed by fitness trackers were on display when a university student used publicly available tools to monitor the movement of military and intelligence personnel at highly sensitive military installations and through the same determine the exact location of these installations.[6] The discovery was part of a much larger privacy breach through a software that produced a global GPS-based heat map of fitness tracker users and could also be used to identify particular individuals through their social media presence.[7]

The scandal highlighted the privacy invasions that were possible due to such devices and the requirement of extensive privacy legislation to ensure users are protected from such invasions in the future. With privacy becoming an increasingly large concern in India, it is important to analyse the privacy risks posed by these devices as well as the protections afforded to citizens. Hence, the paper analyses challenges to privacy

[2] Akanksha Rana & Noor Zainab Hussain, *Google taps fitness tracker market with $2.1 billion bid for Fitbit,* Reuters, available at https://in.reuters.com/article/6us-fitbit-m-a-alphabet/google-taps-fitness-tracker-market-with-2-1-billion-bid-for-fitbit-idINKBN1XB47G, last seen on 14/12/2019.

[3] Nidhi Singhal, *India emerges third largest wearable market in Q2, 26019,* Business Today, available at https://www.businesstoday.in/technology/news/india-em6erges-third-largest-wearable-market-in-q2-2019/story/377302.html, last seen on 14/12/20196.

[4] F. Arriba-Pérez, M. Caeiro-Rodríguez, J. Santos-Gago, *Collection and Processing of Data from Wrist Wearable Devices in Heterogeneous and Multiple-User Scenarios*, US National Library of Medicine, available at https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5038811/, last seen on 05/01/2020.

[5] E. Vogels, *About one-in-five Americans use a smart watch or fitness tracker*, Pew Research Center, available at https://www.pewresearch.org/fact-tank/2020/01/09/about-one-in-five-americans-use-a-smart-watch-or-fitness-tracker/, last seen on 12/01/2020.

[6] L. Sly, *U.S. soldiers are revealing sensitive and dangerous information by jogging*, The Washington Post, available at https://www.washingtonpost.com/world/a-map-showing-the-users-of-fitness-devices-lets-the-world-see-where-us-soldiers-are-and-what-they-are-doing/2018/01/28/86915662-0441-11e8-aa61-f3391373867e_story.html, last seen on 05/01/2020.

[7] K. Leetaru, *Mapping Spies Through Fitness Trackers And Phones: Privacy Is Dead Even For Those In the Shadows*, Forbes, available at https://www.forbes.com/sites/kalevleetaru/2018/07/20/mapping-spies-through-fitness-trackers-and-phones-privacy-is-dead-even-for-those-in-the-shadows/#3acaadc43681, last seen on 05/01/2020.

raised by fitness trackers and the approach used by existing and proposed legal frameworks to protect citizens from these challenges.

## II. DEFINING THE SCOPE

King defines wearable technology as wearables that are augmented or manufactured using technology.[8] This makes the scope of wearable technology broad; including a host of fabrics synthesized or fabricated using technology. These may or may not provide any added functions to the wearable itself. This definition can be further narrowed by requiring smart wearables to provide users with additional information or entertainment, or collecting data through various sensors. Wearable technology can have two further sub classifications namely Wearable Computers and Smart Textiles.[9] Wearable computers refer to miniaturized computers which can be worn in the form of an accessory on one's person. Smart textiles on the other hand refer to fabrics which can measure parameters in the environment around them owing to either electronics or their natural properties. This research focuses on the ability of wearables to measure parameters while not necessarily interpreting or displaying the data measured on the device itself. Smart textiles therefore form an integral part of the paper, however, the data collection elements in wearable computers are also included.

The paper further narrows its scope to focus on applications of wearable technology which collect information relevant to a patient's health and bodily functions. Healey defines four categories of networked medical devices.[10] The first are consumer products which monitor health: these may include other functionalities but must measure one or more of the wearer's bodily functions such as heart rate or steps walked. These are off-the-shelf, commercially sold products which are often linked to smartphones to display parameters measured. Earlier versions of such watches or bracelets may fall under the category of smart textiles as these merely have sensors, whereas newer versions are often wearable computers which can execute several processes. The second category is wearable medical devices. These are devices that are worn on the body with wireless connectivity that may execute a prescribed medical function to ensure the user remains healthy. These devices are usually highly

[8] M. King, *Six Human Factors to Acceptability of Wearable Computers*, Queensland University of Technology, 2011, available at https://eprints.qut.edu.au/50948/1/Madeleine_King_Thesis.pdf, last seen on 04/01/2020.
[9] T. Page, *A Forecast of the Adoption of Wearable Technology*, 6(2) International Journal of Technology Diffusion 12, 13 (2015).
[10] J. Healey, N. Pollard, B. Woods, *The Healthcare Internet of Things*, Atlantic Council, available at https://www.atlanticcouncil.org/wp-content/uploads/2015/03/ACUS_Intel_MedicalDevices.pdf, last seen on 20/12/2019.

specialised in the function they execute and are often worn by users for whom it is medically necessary. This is unlike the first category of products which are often bought to remain health conscious even if not medically necessary. The third categories of products are internally embedded medical devices which reside inside the body of the user, are connected wirelessly and perform a specialised medical function. These include devices such as modern pacemakers. These are normally medically necessary and inserted only by doctors when essential. The fourth categories of networked medical devices are stationary medical devices such as home-care ECG machines which are connected to the internet or other communication networks.

To limit the scope of this research, the intersectionality of networked medical devices and wearable technology will be studied. Using the classifications given by Healey and Page of the two above-mentioned product categories respectively, category one of networked medical devices which have fitness tracking functions of smart textiles will be studied.[11] This constitutes consumer-oriented fitness trackers that can be connected to smartphone applications or other networks and measure one or more health parameters. These devices will be grouped under the categorization of consumer-oriented fitness trackers for the study.

These devices are usually wrist-worn, watch or bracelet like devices available commercially. There are several new devices which include vests that track bodily functions, many of which are being used by professional athletes and their teams to monitor performance. The commercial sale and affordability of such devices is still limited, yet the paper will attempt to include them in the study as well. The innovation in this field is still booming and the market for these devices is predicted to grow in the future.[12]

## III. HEALTH DATA COLLECTED BY POPULAR TRACKERS AND PRIVACY POLICY

Health-related data needs to be processed to provide insights to users themselves and can also be of great aid to medical research. De-identified data from these trackers provided to medical professionals for research can be used to prompt great advancements in the field. Researchers have previously used such data to track diverse parameters such as cardiac

[11] Wearable computers which are housed in accessories such that the accessories have sensors to measure health parameters are also included in the study. The functions of the device which correspond to smart textiles, that is the functionality which allows for measurement of the parameters, are taken into consideration.

[12] J. Jose P., *Smart fabrics: The thread goes tech*, The Hindu Business Line, available at https://www.thehindubusinessline.com/specials/technophile/smart-fabrics-are-poised-to-change-the-clothing-industry/article26934897.ece, last seen on 05/01/2020.

surgery recovery practices and diabetes onset analysis.[13] However, such data is also of great value to several other companies. It is therefore important to assess the privacy concerns arising from the collection of both health and non-health data on these trackers.

| Category | Xiaomi | Apple | Fitbit |
|---|---|---|---|
| Data Collected | - Activity and Sleep<br>- Heart Rate | - Activity and Sleep<br>- Heart Rate<br>- Heartbeat (ECG grade)<br>- Fall detection | - Activity and Sleep<br>- Heart Rate<br>- Heartbeat<br>- Ovulation cycles |
| Privacy Protection | Claims that it abides by principles of necessity and explicit consent in data collection and that data is not processed for any purposes other than those declared to the user.<br><br>Allows users to unsubscribe from the collection of any particular data although warns users that | Stresses on the concept of informed consent, asking for permissions with clear explanations of the sensors being used.<br><br>Claims that it does not share data with any third-party services for any marketing unless the user asks it to. The data collected for the improvement of third-party | Fitbit's privacy policy allows them to sell de-identified user data to third-parties for processing. These are often sold as aggregated non-personal information for research insights. |

[13] S.F. Deangelis, Patient *Monitoring, Big Data, and the Future of Healthcare*, Wired, available at https://www.wired.com/insights/2014/08/patient-monitoring-big-data-future-healthcare/, last seen on 07/01/2020.

| | | | |
|---|---|---|---|
| | it may lead to certain services being discontinued. | applications is collected with consent | |
| Gaps in Privacy Policy | Disputes to be settled in Chinese courts which do not have high privacy protection standards.<br><br>Uses data for advertising, including health related data.<br><br>Does not clarify what happens with data in event of a merger.[14] | Shares data with the company's affiliates.[15] | Fitbit app does not allow users to delete individual parameters, rather one can only choose to delete or keep certain categories of data.<br><br>The default setting on the device is to collect and use all possible data. |

The greatest issue with wearables arises from the amount of data that is being captured on these devices. As discussed above, several these devices have access to a wealth of real-time health and other related data about users which effectively can be used to generate health profiles of each user if data is not de-identified. The revelation of personal health data could have both financial and psychosocial harms for users.[16] Financial harms include denial of insurance or higher insurance premiums, loss of job and inaccessibility to jobs in certain sectors.[17] Psychosocial harms include stigmatisation of the individual and exclusion from communities based on health data obtained, a practice prevalent in India. Data obtained through such platforms can be used to discriminate

[14] Ibid.
[15] *Privacy Policy*, Apple.com, https://www.apple.com/legal/privacy/en-ww/ last seen on 06/01/2020.
[16] J. Lane, C. *Schur, Balancing Access to Health Data and Privacy: A Review of the Issues and Approaches for the Future*, 45 Health Services Research 1456 (2010).
[17] Ibid.

in the provision of public health services to certain communities or persons.

Internet of Things (**"**IoT**"**) devices such as wearables present new challenges to traditional approaches to privacy which need to be tackled as well. It is important to understand that the nature of the device and the nature of the data collected put together demand a rethink of some principles of privacy which are uniformly applied to devices while making policy.

A concept vulnerable to ineffectiveness in the IoT domain is notice and consent. Notice and consent are an integral part of several privacy frameworks including the proposed Personal Data Protection bill. However, most fitness trackers track a variety of parameters continuously which challenges the notice and consent model. If consent is to be taken for every data set captured with notice, it would lead to a high volume of notices which would lead to consent fatigue in users. Consent fatigue refers to users being overwhelmed by the volume of consent requests and leading to users not paying attention to the notice while giving consent. The former Chairwoman of the Federal Trade Commission also questions:

> *Will consumers understand that previously inert everyday objects are now collecting and sharing data about them? How can these objects provide just-in-time notice and choice if there is no user interface at all? And will we be asking consumers to make an unreasonable number of decisions about the collection and use of their data?*[18]

A vital issue with the notice and consent model in the healthcare sector is ensuring consent is informed. Often, users do not understand the extent of information that can be gleaned about them by processing the data they have consented to give. This lack of comprehension is pronounced in the healthcare sector as subject knowledge is required to fully assess the potential of data that a user consents to give. The US President's Council of Advisors for Science and Technology also noted that the notice and consent structure fail in the face of big data, the very kind that is being collected by these devices.[19]

The notice and consent model also seek granularity of consent to be effective. If the privacy structure obtains consent for multiple functions through a singular form, the user has little control over the nature of data they permit to be collected. It turns into a situation where a user is forced

[18] A. Thierer, *The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation*, 21(2) Richmond Journal of Law and Technology 6 (2015).
[19] Ibid.

to choose between consenting to the collection of a large variety of data or not using the service at all. Even though some companies have implemented granularity of consent in their designs, several privacy policies still fall short in this regard. Currently, consent is obtained for a large variety of health data through a single consent form. This makes the user decide between offering up large chunks of health data or not having access to a multiplicity of services at all.

A privacy issue common to most devices is ensuring irreversible de-identification of data. De-identification of data refers to the process of decoupling data about a user from the personal identifiers that may be used to identify a user. This issue is vital in allowing user generated data to inform medical research. Even if extensive health data is being collected about a user, it is not particularly damaging if the data cannot be linked back to the individual who generated it. This will allow for the generation of trends but will prevent profiling. Most fitness band companies collect a wealth of personal data about users in addition to health data and security measures must be used not just at the company server level but also with third party processors to ensure the two data sets cannot be correlated.

Privacy in healthcare also faces the challenge of users not being able to verify enforcement of privacy policies as advertised by service providers. While governments have begun implementing regulatory measures to conduct compliance verification, users in countries where this has not occurred are left in the dark. The issue is exacerbated with medical data due to a lack of user knowledge on the backend mechanisms for storing and sharing such data and not enough information being available about third-parties processing the data.[20]

Several wearable devices in the market have voice command functions enabled on them. These allow the microphone to be on at several times through a single consent form obtained from the user at the time of configuration. Due to this, such devices pose a threat to bystander privacy.[21] While users themselves may have consented to allow their conversations to be overheard by the device, bystanders may not have entered into the same consent agreement with the company. However, by having the microphone or other such sensors functioning, the device may detect information about bystanders that may violate their privacy. This maybe the case even in private spaces where there is a reasonable expectation of privacy that the bystander has. This issue is complicated by

[20] S. Haas, S. Wohlgemuth, I. Echizen, N. Sonehara, G. Mueller, *Aspects of privacy for electronic health records*, 80 International Journal of Medical Informatics 26, 31 (2011).
[21] P. Dutta, M. Chatterjee, A.S. Namin, *A Survey of Privacy Concerns in Wearable Devices*, IEEE International Conference on Big Data (2018), available at https://ieeexplore.ieee.org/document/8622110, last seen on 07/01/2020.

the fact that companies are trying to make smart textiles and wearables indistinguishable from regular accessories. Hence, for bystanders these inadvertently become concealed recording devices which pose a significant privacy threat. Manufacturers and data processors need to take steps to ensure that bystander data is filtered out and data collected is limited to the individual who has given consent.

These issues cannot be resolved by institutional regulation alone. It requires user awareness which will prompt companies to enhance their privacy and security standards. However, bringing user awareness in specialised areas such as health data collection continues to be a challenge which needs to be overcome. Additionally, the value of such data for research cannot be ignored and overregulation could lead to companies not sharing data for crucial medical research. A nuanced approach to protecting personal data while allowing for research through de-identified data or informed and explicit consent needs to be used in regulation of the space.

## IV. LEGISLATION AND REGULATION IN INDIA

In 2018, in a landmark judgement, the Supreme Court adjudicated that the Right to Privacy is a protected fundamental right of Indian citizens under Articles 14, 19, and 21 of the Indian Constitution.[22] Since the judgement, there has been a renewed focus in New Delhi on creating legislation to protect the right to privacy by regulating the digital industry in India. Digital privacy for individuals is still largely protected by the Information Technology Act, however, there has been new legislation proposed to overhaul the frameworks through which data flow is regulated to protect privacy. This section analyses the salient features of the proposed legislation and assesses the protections afforded to citizens by existing legislation. It also tries to reconcile approaches to privacy by a variety of rules that may apply to health data to ensure a uniform, coherent structure that is easy to comply with.

## V. PROPOSED LEGISLATIONS

### 1. Personal Data Protection Bill

The Personal Data Protection (**"**PDP**"**) Bill is a proposed legislation that revamps the digital privacy protection framework in India.[23]The Bill, which has been in the pipeline for some time, was introduced in the Lok Sabha in December 2019 and has been referred to the Standing Committee on Information Technology of the Parliament. A report from

[22] K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
[23] The Personal Data Protection Bill, 2019 (pending).

the Standing Committee is expected in the 2020 Budget Session of Parliament post which the Bill can move forward.[24] The Bill draws inspiration from the General Data Protection Regulation passed in the European Union and follows a similar approach to privacy protection in the digital sphere.

The Bill seeks to establish a regime of data protection wherein data is collected and processed in a manner which is necessary, fair, transparent and requires the consent of the user from whom the data is being collected. The Bill defines several important concepts in digital privacy protection such as de-identification and anonymisation, which gives shape to India's interpretation of these principles.[25] The Bill seeks to create a Data Protection Authority in India which will create regulations and ensure standards are maintained for the protection of data. The Bill defines the mandate of the Authority and the powers it will have when created.[26]

The Personal Data Protection Bill is an overarching piece of legislation that covers most data generated, collected and processed in India. The scope of the Bill is beyond Indian jurisdiction alone and covers data generated by Indian citizens which may be stored or processed overseas. The Bill is expected to regulate most forms of data while ensuring sectoral regulators are consulted in the implementation of codes and regulations for sector specific data.[27]

### 2. Digital Information Security in Healthcare Act (DISHA)

The Digital Information Security in Healthcare Act, known commonly by its abbreviation, DISHA, was released by the Ministry of Health and Family Welfare.[28] The regulation was released for public consultation in March 2018 with comments invited on the document. There has been little progress with the Bill, which could have been delayed to ensure it is in line with the Personal Data Protection Bill.[29]

The Bill governs Electronic Health Data collected in India and places data protection regulations on medical establishments and other entities collecting such data. It also seeks to create a network of Digital Health

[24] *The Personal Data Protection Bill, 2019*, Parliamentary Research Service, India, https://www.prsindia.org/billtrack/personal-data-protection-bill-2019, last seen on 05/01/2020.
[25] Supra 25.
[26] Ibid.
[27] Ibid.
[28] Digital Information Security in Healthcare, Act, 2018 (pending).
[29] S. Agarwal, P. Raghavan, *Health Ministry may await DISHA from BN Srikrishna report*, Economic Times, available at https://economictimes.indiatimes.com/tech/internet/health-ministry-may-await-disha-from-bn-srikrishna-report/articleshow/65098136.cms, last seen on 09/01/2020.

Authorities, with a nodal national authority and several state authorities.[30] The Act was one of the first proposed legislations in India to define the rights of data owners and limit the scope of collection and processing of health data. The Act also hinges on a notice and consent model, akin to the PDP Bill.[31] The Act is focused on health data collected at clinical establishments, but widens its scope to additionally cover other forms of health data generated.

### 3. Reconciling the Personal Data Protection Bill and the Digital Information Security in Healthcare Act with regards to regulations on consumer-oriented fitness trackers

Owing to the definitions put forth in both regulations, there appears to be an overlap in the nature of data being covered. Both regulations define a variety of data and have separate definitions of health data as well which leads to a regulatory overlap. Due to this, it is important to analyse the nature of regulations these two legislations impose on health data and if they are reconcilable. It is crucial to do so to understand the breadth of regulations that govern health data produced by consumer-oriented fitness trackers.

Both sets of regulations have definitions of health data that could be interpreted as applying to health data produced by consumer-oriented fitness trackers. The Personal Data Protection Bill includes "data related to the state of mental and physical health of the data principal" as well as data collected in the course of provision of health services in its definition of the term "health data".[32] This could be interpreted as covering the data produced by fitness trackers as most contain data that is related to the physical health of the user and is used to provide a health service as well. DISHA covers the two above-mentioned forms of data as well "information derived from the testing or examination of a body part" in its definition of Electronic Health Data.[33] Hence, it could be easily construed that DISHA covers most health data produced by fitness trackers as well. Besides, the PDP Bill also covers health data within its definition of Sensitive Personal Data, bringing fitness tracker health data under the ambit of the category as well.[34]

The PDP Bill has certain provisions which will apply to most categories of personal data collected by fitness trackers, as well as other provisions for health data and sensitive personal data which will apply to certain sub-

[30] Supra 26.
[31] Ibid.
[32] Supra 25.
[33] Supra 26.
[34] Supra 25.

categories. Unlike DISHA, which only covers the health data components of data collected by fitness trackers, the PDP Bill governs elements of non-health related personal data that these trackers collect as well. Specifically, the Bill has provisions to ensure that necessary provision of health services is not blocked and that sensitive personal data such as health data puts a higher burden on companies than personal data.[35]

The PDP Bill does not bring under its mandate the regulation of anonymised data.[36] Hence, companies are free to use anonymised data from fitness trackers for advertising, transfer to third parties and other commercial purposes. This means that any data from which the personal identifier fields are encrypted or masked, can be used to analyse trends on location, health and application usage under the Bill. The Bill operates on a notice and consent model with descriptive conditions on the nature of notice that is to be given and how consent can be obtained. The Bill however sets out several exceptions to the requirement of consent for data processing. The data collector or processor is exempted from obtaining consent to respond to a threat to life or medical emergency of any individual.[37] This exception does not cover sensitive personal data, which means fitness trackers cannot use this exception to process health data of the individual without consent but may access data such as location or home address to respond to a medical emergency. If the data collector is the employer of the data principal, they can use personal data to recruit or terminate the data principal as well.[38] The Bill also ensures that consent does not restrict governmental agencies from accessing personal data.

The first recommendatory reports for the PDP Bill suggested a requirement of data localisation on all personal data. This meant that a copy of all personal data of Indian citizens had to be stored in the physical territory of India. However, the most recent iteration of the Bill imposes this requirement only on sensitive personal data.[39] This means that fitness tracking companies will have to store copies of health data collected on fitness trackers in local data centres when the Bill comes into effect and can only transfer the data overseas for processing when explicit consent for the same is obtained from the data principal. The Central Government shall form rules on codes of processing and storage of sensitive personal data.

[35] Ibid.
[36] Ibid.
[37] Ibid.
[38] Ibid.
[39] Ibid.

While the PDP Bill has overarching regulations for a variety of data, which are also applicable to data collected on fitness trackers, DISHA expressly regulates digital health data. Large parts of the legislation govern data from clinical establishments and health information exchanges; however, by bringing "entities" which include registered companies collecting health data into the ambit of the legislation, fitness tracking companies can be interpreted to be included. DISHA outlines a digital data protection model through a rights-based approach for data owners.[40] It affords data owners several rights which give them protections against the misuse of their data and breaches of privacy. Under these rights, the owners of data have the right to refuse consent from data being generated altogether.[41] For fitness trackers, this would mean that while this data cannot be collected, it also cannot be recorded at the first instance by the sensors within the device if the relevant section is interpreted such.

A key issue with the DISHA regulations is that they prevent health data being collected on fitness trackers from being used for medical research.[42] It allows only for electronic health data captured by clinical establishments to be used for any academic research and does not allow data captured by other entities to be used for this purpose under Section 29[43]. Even for clinical establishments, it allows such research to be done only with de-identified or anonymised data with no personal identification permitted. The legislation protects data of users from being used for commercial purposes, disallowing the same even if consent is obtained.[44] The legislation expressly disallows insurance companies from insisting to access data for clients purchasing health insurance if the user does not consent to the same. DISHA imposes significant penalties on entities failing to comply with the rules and if put into effect will help strengthen the privacy protections on health data afforded to users.

## VI. ASSESSING CONCEPTUAL DIFFERENCES IN THE LEGISLATIONS PROPOSED

The two bills differ in defining several other salient concepts as well, which when applied concurrently may cause compliance issues for companies. DISHA defines anonymisation as "the process of permanently deleting all personally identifiable information" from an individual's records.[45] On the other hand, the PDP Bill defines anonymisation as an "irreversible process of transforming or converting

[40] Supra 26.
[41] Ibid.
[42] Ibid.
[43] Supra 28.
[44] Ibid.
[45] Ibid.

personal data to a form in which a data principal cannot be identified".[46] While the definition of anonymisation under the PDP Bill only requires an irreversible de-linking of data sets which serve as personal identifiers from other personal data, DISHA requires companies to delete all personal data altogether when implementing anonymisation. The regulations on anonymised data in the two bills also differ. The PDP Bill excludes anonymised data from the purview of the regulations under the Bill and does not regulate such data at all. On the other hand, DISHA in Section 29(5) mandates that even anonymised digital health data cannot be accessed for commercial purposes and by insurance companies, pharmaceutical companies or employers.[47] Hence, it may be construed that while the PDP Bill allows anonymised data collected from fitness trackers to help advertisers with directed advertising, DISHA does not allow even anonymised data to be used for this purpose as it is "commercial" in nature.

The notice and consent model is distinct in these two legislations. DISHA defines consent as "expressed informed consent given by the owner after understanding the nature, purpose and consequences of the collection, use, storage or disclosure of the digital health data".[48] The PDP Bill has a more elaborate definition of consent, employing certain tests to ensure that the data principal is giving informed consent. The PDP Bill requires consent to be free,[49] informed,[50] specific,[51] clear, and capable of being withdrawn.[52] Additionally, the PDP sets a higher standard for consent for Sensitive Personal Data, which includes health data. The Bill requires data processors, before obtaining consent, to inform principals of any processing that may cause significant harm to the principal. After giving the principal the option to consent separately to sharing various kinds of sensitive personal data, it provides granularity of consent.[53] The PDP Bill also places the burden of proof for showing that the consent was obtained on the party collecting the data and not on the user.

While the PDP Bill may have a more descriptive definition of consent, DISHA gives the data owner several consent-oriented rights. DISHA

[46] Supra 25.
[47] Supra 26.
[48] Ibid.
[49] Complying with the standard of 'free' specified in Section 14 of the Indian Contract Act, 1872.
[50] Informed consent can only be given when the data principal has been provided with the requisite data under Section 7 of the same bill. This includes information about what kind of data is being collected, who is processing it, how the data is transferred, how long the data is retained and the purpose for processing the data among others.
[51] Specific consent means that the data principal should understand the scope of data he or she is giving consent for through that particular consent form.
[52] Supra 25.
[53] Ibid.

administers granularity of consent to data owners in a different manner than the PDP Bill. DISHA allows for the data owner to provide or withdraw consent at each step of the data flow, a feature missing in the PDP Bill. DISHA requires data collectors to obtain consent separately for collecting the data, storing the data, transferring the data, access of data by a third-party, and disclosure of data.[54] The legislation also ensures that if the data owner refuses to consent to one of the steps in the data flow, the services that can be provided despite that denial of consent must be provided. This means that if the data owner refuses to consent to data being transferred to a third-party, the health services that can be administered by the collector independent of the third-party must not be refused based on that denial of consent. On the other hand, the PDP Bill requires data collectors to notify the owner of most elements of the data flow, it however, does not give owners the right to refuse consent to individual steps of the data flow.[55] DISHA also mandates that separate consent be required before every individual use of the owner's data, whereas the PDP Bill allows companies to take a one-time consent for a certain kind of data from the owner. DISHA also gives users greater rights in withdrawal of consent than the PDP Bill. DISHA effectively gives users the right of erasure of data on them. This means that the user can not only withdraw consent from further collection of data but can also withdraw consent for stored data. In this circumstance, the data would need to be deleted which would mean that processing which may fall outside the consent-based model in the regulation will also not be possible. An example of processing which may fall outside the consent-based model is access to data by law-enforcement agencies. If the owner withdraws consent from the storage of data, all copies need to be deleted and hence cannot be accessed by law enforcement agencies as well. The PDP Bill does not give the same right. The PDP Bill allows only for the user to disallow disclosure of data, however, exceptions to this withdrawal of consent are also laid out under the Bill.[56] It has provisions allowing for retention of data for a certain period. Additionally, the Bill does not give granularity of consent for individual steps of the data flow, hence the data principal can withdraw consent for the collection and processing of data from that point onwards but can do very little to limit storage of data already collected in the past about them.

The two sets of regulations impose different standards for governmental access to data as well. DISHA imposes a much higher burden on government agencies for access to health-related data. Government agencies can only access data in de-identified or anonymised form and

[54] Supra 26.
[55] Supra 25.
[56] Ibid.

cannot access personal identifiers related to the health data collected.[57] The purposes for which this data can be collected is also limited under the provisions set out by Section 29 of the rules. Section 29 allows this kind of data to be used for research and policy planning, to prevent public health emergencies, to assess the quality and effectiveness of healthcare facilities, and to prevent bioterror events and infectious disease outbreaks.[58] The Government agency requesting the data has to lodge a formal request with the National Electronic Health Authority only after which they will be permitted access to data. While the provisions for preventive assessment still leave room for the government to access data on various pretexts, the fact that only anonymised data can be accessed is a significant departure from previous laws in the degree of protection afforded to data owners. However, the National Electronic Health Authority's members are appointed by the central government of which some are ex-officio civil servants in certain ministries.[59] This may lead to a dilution of the independence given to the Authority and may reduce some of the protections given to users. Despite this, the legislation sets unprecedented protections for users on governmental access to data. The only mechanism under the Rules through which personally identifiable health data may be accessed by the government or law enforcement agencies is when a court order to access such data is granted for a cognizable offence. Hence, law enforcement agencies cannot access such data without filing for a warrant with the judiciary which puts a check on abuse of power by law enforcement agencies in this regard.

The PDP Bill, on the other hand, gives the government a range of powers for processing personal data without requiring consent of the data principal. The government is allowed by the Bill to process personal data to provide any public services to individuals or for the issuance of licenses to individuals. The governments, as well as others, are permitted to process such data to provide assistance in the event of a disaster or to provide medical assistance in the event of a disease outbreak.[60] The government is also allowed to determine what data constitutes sensitive personal data. Even though the Bill lays out certain kinds of data as sensitive personal data in its definition, the government has the power to specify whether certain kinds of data fall under the category of sensitive personal data. Apart from these, provisions under Section VIII of the Bill expressly exempt the government and agencies appointed by it from the protections afforded to data principals under the PDP Bill.[61] The government is authorised to request data from any collector or processor

[57] Supra 26.
[58] Ibid.
[59] Ibid.
[60] Supra 25.
[61] Ibid.

of data if it feels that the data can help the government to prevent the incitement of a cognizable offence. For this purpose, the government does not require even a court order or warrant and merely needs to record its reasons in writing.[62] The government also has the power to authorise other companies to access and process data, including companies incorporated outside India. This permits the government to appoint intermediaries to process data on behalf of the government, with the intermediary being exempt from most protections granted under the law. All of these provisions put together, the government is virtually exempt from the regulations for most forms of data. None of the exemption provisions, however, mention sensitive personal data as being exempted from consent requirements. There is a lack of clarity on how the government will access sensitive personal data. Even though there are no exemption rules for this category, it is almost certain that some of this data will be essential for law enforcement agencies and the government can codify standards for sensitive personal data under Section 15 of the Bill. With health-related data being covered under sensitive personal data, the protections afforded to it against governmental access are not clear.

## VII. EXISTING REGULATIONS APPLYING TO HEALTH-RELATED DATA ON FITNESS TRACKERS

### 1. Information Technology Act 2000 (amended by IT (Amendment) Act 2008)[6364]

The IT Act is currently the legislation which forms the backbone of data protection regulations in India. It defines offences and penalties for breaches of data privacy and failure to protect data. The Act defines the "failure to protect data" and mandates compensation by companies who have been adjudicated to be negligent in handling of sensitive personal data which led to a data breach which caused harm to individuals.[65] Under the Act, the central government can decide on what data it deems must be categorised as sensitive personal data. The Act was also one of the first in India to take note of and use the notice and consent model for privacy in 2000.[66] It defined the disclosure of electronic records obtained without the consent of the owner as an offence. The Act also criminalized unauthorised access to computer systems and networks as well as unauthorized extraction of information from a computer.[67] The Act is the existing general body of rules for data protection which are

[62] Ibid.
[63] Information Technology Act, 2000.
[64] Information Technology (Amendment) Act, 2008.
[65] Supra 64.
[66] Ibid.
[67] Ibid.

augmented by sector specific regulations. The PDP Bill is set to revamp privacy protections for data under the IT Act.

Subsequently, the Government framed a set of rules under Section 87 of the IT Act. These rules, titled the "Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011"[68] lay a standard for data protection measures to be taken by data collectors and processors. The Rules brought medical records under the purview of Sensitive Personal Data as well as including physical, physiological and mental health condition.[69] This brings the health data recorded by fitness trackers under the mandate of the Rules. The Rules enforce a condition of necessity for data collection. They also elaborate on the notice and consent model mentioned in the IT Act. The Rules require notification to the data owner of information being collected, the purpose of the collection and the intermediaries that information is shared with.[70] The Rules also require the company to take explicit consent of the owner and gives the owner the right to withdraw consent at any time for the collection of data. The Rules require companies to obtain consent of the data owners for transferring their data to a third party.[71] The Rules also require the third party to have the same standards of data security as the company collecting the data. The Rules lay down other principles of data protection, such as requirements that information can only be processed for the purpose it was collected and that information should not be retained longer than required.[72] Finally, the regulation sets standards of system security to be followed by the data collector and sets out a mechanism to audit the same. As the definition of sensitive personal data under the Rules covers health-related data collected by fitness trackers, they fall under the purview of the Rules.

### 2. Electronic Health Record Standards (2016)[73]

The Electronic Health Record Standards are sector-specific regulations on the storage of electronic health records put forth by the Ministry of Health and Family Welfare. They specify requirements of healthcare data as a sector-specific add-on to the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011. The Standards are recommendatory and are not legally binding.[74] The Standards acknowledge the popularity of self-care

[68] Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.
[69] Ibid.
[70] Ibid.
[71] Ibid.
[72] Ibid.
[73] Electronic Health Record Standards, 2016.
[74] Ibid.

health devices that continually produce data and note that these also constitute essential healthcare data.[75] The Standards define a category of data named electronic Protected Health Information which includes data about the past or present mental or physical health condition of an individual which is stored electronically. They confer ownership of healthcare related data which comes under sensitive personal data in the IT Rules, 2013 to the individuals from whom data is collected.[76] They also give the patients the right to restrict disclosure or access to their data and to view the data that organisations have about them. Even though anonymisation and de-identification are not defined as such, the standards recommend all healthcare data collectors to remove personal identifiers where not required.[77] The Standards also recommend granularity of consent, wherein a patient can request that specific elements of their information not be disclosed or be accessible by third parties. The recommendation also establishes data security standards that should be implemented by providers who store electronic health records.[78] They suggest healthcare providers to follow a set of global standards including various ISO standards on health informatics as well as encryption standards. The document emphasizes on the link between data security and data protection and considers data security as a necessary element of assuring data protection for companies.[79] These standards are also applicable to fitness trackers as the recommendations acknowledge self-care health devices as a part of the ambit of the recommendations. However, by virtue of them being recommendations, there is no enforceability and hence they may only shape privacy policies of companies.

## VIII. CASE LAWS

It is also crucial to analyse the view that the Indian judiciary has taken in the matter. There exists case law to determine the Indian judiciary's view on the question of privacy in health-related data which has often been weighed against public interest. Through such cases, precedence has been created on issues to be considered while evaluating whether privacy of health data overrides the public interest.

### 1. K.S. Puttaswamy v. Union of India (2017)[80]

The judgment delivered in this case is considered a landmark as the Supreme Court manifestly declares the Right to Privacy as a fundamental

[75] Ibid.
[76] Ibid.
[77] Ibid.
[78] Ibid.
[79] Ibid.
[80] Supra 32.

right under the Indian Constitution. The Court makes several references and expresses beliefs regarding the privacy protection extended to medical information in the judgement. The Court ruled that the Right to Privacy was a natural and inalienable right of all humans. The judgement reads, *"Privacy of the body entitles an individual to the integrity of the physical aspects of personhood"*. This statement can be read to include physiological information about the body of the nature that is tracked by fitness trackers, bringing them within the ambit of the Right to Privacy. The judgement also acknowledges "Informational privacy" as a type of privacy, recognising the right of an individual to control dissemination and access to information concerning them. Under the concept of informational privacy, the Court expressly makes note of challenges arising from wearable devices. The judgement acknowledges that with such devices, users often cannot understand the vast amounts of data they have volunteered. The Court also manifestly declares that it believes that users have a reasonable expectation of privacy with data such as medical information. It also chooses to elaborate of anonymity in the sphere of health-related data. The Court expresses its belief that while personally identifiable data may not be accessed, there may be access to anonymised data for informing public health decisions. Put together, these statements exhibit the Court's belief that users have a reasonable expectation of privacy over their medical information and that the violation of privacy for such data has a relatively high burden as compared to other forms of data.

### 2. Mr X v. Hospital Z (1998)[81]

In this case, the Supreme Court questioned whether it was a breach of the right to privacy and confidentiality of an individual if their HIV Positive status was revealed by a hospital, tested during transfusion, to the person they were to be married to. In the 1998 judgement, the Supreme Court held that the right to privacy is not absolute and may be restricted for the prevention of crime or protection of health. It ruled that the Right to Privacy of the HIV Positive individual had not been affected in disclosing the information to the family of the spouse. The Court viewed the health of the would-be spouse in high regard and maintained that the disclosure done to protect the would-be spouse from HIV did not infringe on the Right to Privacy of the infected individual. This case promulgates a trend in several other cases where the courts have held information disclosed in public interest to not be a violation of the right to privacy. It is to be noted, however, that the Court referred to Kharak Singh v. State of U.P. and Gobind v. State of M.P. in tracing the right to privacy, which K.S. Puttaswamy v. Union of India builds on.

[81] Mr. 'X' v. Hospital 'Z', (1998) 8 SCC 296.

### 3. Sharda v. Dharmpal (2003)[82]

In this matter, the Supreme Court was called upon to decide, among other questions, whether the courts could subject an individual to a medical examination. The case involved a married couple of whom the respondent was filing for divorce because the appellant was not sound of mind. The lower court had asked the appellant to submit themselves to a medical examination and submit the findings as evidence in the matter. The appellant appealed to the Supreme Court claiming that the courts could not order a medical examination as it would be a violation of the appellant's privacy. The Court acknowledged that the medical information obtained from the test would be instrumental in concluding the case, but questioned whether obtaining such medical information would violate the appellant's right to privacy. In the judgement, the Court held that the Right to Privacy under Article 21 of the Constitution is not absolute. Since the Right to Privacy is not absolute, the court held that if two parties had fundamental rights in conflict with one another, the right which advances public morality would prevail. The Court held that an order for a medical examination would not be violative of the individual's right to privacy. This is because the Court believed that the case could not reach a fair conclusion without this data and added that only data necessary for delivering the judgement must be collected. The Court in its ruling also acknowledged that under certain laws the State has the right to subject an individual to a medical examination. Presumably, if the law can subject the individual to an examination, accessing data that would give the same information as the examination itself must also be permitted. The case highlighted the limitations of the Right to Privacy under Article 21 of the Constitution on medical information. However, K.S Puttaswamy v. Union of India brings the Right to Privacy within the ambit of Articles 14 and 19 of the Constitution as well. Keeping that in mind, in subsequent cases of this nature, the question of conflicting fundamental rights may need to be revisited in the case of the Right to Privacy.

## IX. CONCLUSION

Current Indian legislation is found wanting in the domain of data protection for fitness trackers. The existing legislation has limited intent to protect privacy of citizens, being more focused on preventing cyber-crime and ensuring cyber security. The IT Act and rules under it do lay the groundwork for creating protections for health-related data however, defining sensitive personal data and criminalising breaches of privacy. They also impose responsibilities on companies collecting personal data

[82] Sharda v. Dharmpal, (2003) 4 SCC 493.

of citizens by penalising them for breaches where the company is found negligent in its storage of data. In recent years, following the General Data Protection Regulation in the EU and the Justice Puttaswamy judgement by the Supreme Court, the Indian government has displayed an intention to create legislation for data protection. The Electronic Health Record Standards (2016) by the Ministry of Health and Family Welfare acknowledge the necessity of creating rules for data protection and recognise the pervasiveness of self-care medical devices. In doing so, it creates the framework which is then used by proposed legislations to ensure data protection for health data.

The Personal Data Protection Bill, while covering a range of data, appears to be lenient towards data protection. Even though it is a significant improvement to India's existing data protection framework, it leaves a lot to be desired when looking particularly at health-related data. The Bill does not comprehensively cover the additional protections offered to sensitive personal data over personal data and in doing so leaves several questions over the protection of such data unanswered. The Bill uses a limited approach to notice and consent and fails to cover several aspects of the same. This leaves the protections extended by the Bill vulnerable to the nature and magnitude of data captured by internet-of-things devices, such as fitness trackers. It is unable to tackle several challenges posed by such devices to traditional notice and consent approaches as mentioned in the paper.

The proposed Digital Information Security in Healthcare Act is markedly more nuanced in the protections offered by it to health-related data than the PDP Bill. It breaks down the data flow to its fundamental processes and ensures that the notice and consent model applies to each stage, granting the data owner significantly more control than the PDP Bill. However, progress on DISHA has stalled, seemingly in anticipation of the PDP Bill. It is imperative, though, that DISHA is passed to provide directed protections to health-related data. An attempt does need to be made to reconcile the two legislations as they have differing approaches to several problems. However, DISHA must not be changed drastically from its present form to accommodate the leniency of the PDP Bill if the protections to healthcare data are to be comprehensive. Rather, DISHA must be treated as specific law and allow the legal principal of *lexspecialis derogat legigenerali,* meaning more specific rules will prevail over general rules, to apply in a conflict between the two laws. The PDP Bill is essential and useful but in bringing a variety of data under its mandate, it cannot extend comprehensive protections to any particular kind of data, which DISHA does.