PROTECTING THE HEALTH DATA OF CONSUMERS: NEED FOR AN IRON-CLAD LAW IN INDIA

— *Ashutosh Tripathi*[*] *and Tushar Behl*[**]

Abstract: *One of the major concerns for all countries presently dealing with COVID-19 pandemic is to strike a balance between the privacy rights of the patients and public health surveillance, which is being done through various apps like* Aarogya Setu *in India, which is needed in the larger interest of the society. Public health Surveillance system although with good intention has to respect the privacy of the people. Supreme Court of India has recognized right to privacy as a part of right to life under the art 21 of the Constitution of India in the* Puttaswamy *judgment.*

In this essay, it is argued that the present legal framework regarding the health protection data in India is not sufficient for protecting the sensitive data of the patients although certain steps have been taken but all are in the forms of the bill, namely, Digital Information Security in Healthcare and Personal Data Protection Bill 2019. The essay will also be looking at some of the best practices in the world regarding the protection of health data mainly that of USA and Australia. The essay explains why India will be well ahead in terms of health protection data if we implement all the laws, which are still at the draft stage.

Keywords: Consumer Protection, Data, Constitution, Health, Privacy, etc.

[*] Ashutosh Tripathi is presently an Assistant Professor of Law-Senior Scale at the School of Law, University of Petroleum and Energy Studies, Dehradun (UPES). He holds a Masters of Law (LL.M.) from NLSIU, Bengaluru, and is also currently pursuing a Ph.D. from NLSIU.

[**] Tushar Behl is a law graduate from the School of Law, University of Petroleum and Energy Studies, Dehradun (UPES).

I. INTRODUCTION

The continuous proliferation and evolution of new technologies expose the electronic health records (hereinafter 'EHR') of consumers, to an inordinate risk. Conceivably, it is the digital health data (hereinafter 'DHD'), containing the personal health information of patients, which is vulnerable to serious risks of privacy and security.[1] While the use of DHD was promising enough to revolutionize the healthcare system in India, in addition to the personal information supplied voluntarily, online behavior tracking is on the verge without informed consent of consumers.[2]

The porous interface between right to privacy and the need for medical treatment makes personal health data protection, a prime concern. A patient's personal health information from his first admission/attendance at the hospital, to his final laboratory tests is entered and stored online at the point of care over the patient's lifetime. The information is readily available and accessible by all healthcare providers in charge of the patient, however, the extent and nature of data collection is totally unprecedented. Not to forget, the potential risks which can arise when this information is pooled with other sources like drug companies, leading to manipulative marketing, data breaches, discriminatory profiling and re-selling of personal information in lieu of online trading activities.[3]

Administrative and physical safeguard standards do exit for industries handling medical and personal health information, but certain gaps emerge with

---

1 Fouzia F. Ozair and others, 'Ethical Issues in Electronic Health Records: A General Overview' (2015) (6)(2) PICR <http://www.picronline.org/temp/PerspectClinRes6273-5763666_160036.pdf > accessed 2 April 2020.

2 Stephen Corones and Juliet Davis 'Protecting Consumer Privacy and Data Security: Regulatory Challenges and Potential Future Directions' (2017) 45 Fed L Rev 65.

3 Kathryn C. Montgomery and others, 'Health Wearable Devices in the Big Data Era: Ensuring Privacy, Security, And Consumer Protection' (CDD Report, 2017). <https://www.democratic-media.org/sites/default/files/field/public/2016/aucdd_wearablesreport_final121516.pdf> accessed 2 April 2020.

the advancement of new technologies[4] and it becomes essential that security and privacy standards work closely to craft suitable controls and protections.

A related problem is the use of health-monitoring tools, i.e. wearable fitness technology such as bands, smart watches, pedometers and other wearable ECG monitors.[5] The rising trend in wearable fitness technology revolves around this critical question of how to safeguard a user's privacy, in a better way.

In 2015, The Ministry of Health and Family Welfare (hereinafter 'MoHFW') published a note establishing a National e-Health Authority (hereinafter 'NEHA') to ensure promotion and development of e-health ecosystem in India. Acting on the same vision and mission, the Ministry, in March 2018, ratified the draft of "Digital Information Security in Healthcare, Act (hereinafter 'DISHA') in public domain. The intention behind DISHA was to establish NEHA and other health information exchanges, including the State e-health authorities (hereinafter 'SEHA'), standardizing the process of DHD collection and to ensure the much needed privacy and security of DHD.

India's current regulatory approach to this issue has been to draft its own data protection law, ie Data Protection Bill. The much awaited bill, which started its journey full of controversies, was expected to be approved by the end of 2019, however as one would say, India's first attempt to nationally legislate a promising mechanism for data protection seems to be moving two steps forward and six steps backward.[6] Indian data protection and privacy laws are extremely patchy. This is a big concern when we talk about securing personal health data of a population more than 1.3 billion.

The structure of this note is to consider first, in **Part II**, the current framework pertaining to the existing health data protection legislation in India. **Part III** broadly discusses the international practice of privacy protection, drawing out a comparative analysis with Australia and the United States of America. **Part IV** discusses the constitutional framework and whether India should re-consider strengthening the protection for health information privacy and **Part V** proposes recommendations and modifications to the existing law that may address disquiets concerning privacy and security of individuals.

---

4 Terence M. Durkin 'Health Data Privacy and Security in the Age of Wearable Tech: Privacy and Security Concerns for the NFLPA and WHOOP' (2019) 19 J High Tech L 279.

5 Alicia Phaneuf, 'Latest Trends in Medical Monitoring Devices and Wearable Health Technology' (*Business Insider India*, 19 July 2019) <https://www.businessinsider.in/science/latest-trends-in-medical-monitoring-devices-and-wearable-health-technology/articleshow/70295772.cms> accessed 2 April 2020.

6 Rudra Srinivas 'All You Need to Know About India's First Data Protection Bill' (*CISOMAG*, 3 January 2020) <https://www.cisomag.com/all-you-need-to-know-about-indias-first-data-protection-bill/> accessed 2 April 2020.

II. HEALTH DATA PROTECTION LEGISLATION IN INDIA

The health care industry in India is on the rise and is changing constantly. Personal health data of the patient is in the hand of healthcare institutions. The National Health Policy 2017 suggested creating a digital health technology ecosystem, involving large scale collection, organization and sharing of health data.[7] Health data means the data related to the state of physical or mental health of the data principal and includes records regarding the past, present or future state of the health of such data principal, data collected in the course of registration for, or provision of health services, data associating the data principal to the provision of specific health services[8].

The initial step regarding this ecosystem was taken in 2012 when the government made it mandatory for the clinics to maintain electronic health records of their patients under Clinical Establishment Rules[9]. With this changing landscape, the first thing that strikes into one's mind is regarding the prevention of the disclosure of the personal and critical medical information. Now the question is: *how we strike a balance between security, privacy and development?*

Till date, there is no legislation in India which protects the healthcare data. India took the first step when the Ministry of Health and Family Welfare proposed 'DISHA' (hereinafter 'Digital Information Security in Healthcare Act') in March 2018. DISHA expects to be an enactment concentrated on data protection, secrecy, and security. DISHA aims to make administrative specialists, both at the central and state level, to carry out the rights and obligations as given under the said legislation.

At the central level, the setting up of a National Electronic Health Authority (hereinafter 'NEHA') was proposed, which would be the topmost authority dealing with setting standards, issuing guidelines, and regulating the collection, organization, and transfer of the health data. At the state level, the State Electronic Health Authority (hereinafter 'SEHA') will be answerable for guaranteeing that the necessities of DISHA are followed by the institutions[10]. DISHA is going with the consent based approach, giving significant rights to

---

7 'DISHA and the Draft Personal Data Protection Bill, 2018: Looking at the Future of Governance of Health Data in India' (*Ikigai Law*, 25 February 2019) <https://www.ikigailaw.com/disha-and-the-draft-personal-data-protection-bill-2018-looking-at-the-future-of-governance-of-health-data-in-india/#acceptLicense> accessed 27 April 2020.

8 The Personal Data Protection Bill (2019), cl 3(21).

9 Clinical Establishments (Central Government) Rules 2012, r 9(iv).

10 Milind Antai and others, 'DISHA the First Step towards Securing Patient Health Data in India' (*Mondaq*, 3 August 2018) <https://www.mondaq.com/india/healthcare/723960/disha-the-first-step-towards-securing-patient-health-data-in-india> accessed 27 April 2020.

the owner of the data, where he can decide what should, and can be done to his personal data.[11]

Another draft that was proposed was the Personal Data Protection Bill 2019 which would create the first cross-sectoral legal framework for data protection in India.[12] This bill also deals with protecting the personal data of the individual.[13] This bill is concerned with many other forms of data, one of them being, the health data. The health data comes under the head of 'sensitive personal data'.[14] As the name itself suggests, the data of such special category must be treated with extra care and caution. The authorities under this regime have a duty to protect the data and the principal agent giving the right to access, erase, and correct the personal health information.[15]

Both the bills were introduced for protecting the personal healthcare data, however, these legislations have not been implemented yet. The reason being, the increasing concern regarding security as the principle of privacy; this principle has been developed over a period of past few years. In line of this, the Apex Court propounded that 'The right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21'.[16] In addition, the informational privacy is a subdivision of it.[17]

The present legal provisions dealing with such protection clearly provide that at whatever point a corporate body has or manages any delicate individual information or data, and is careless in keeping up security to protect such information or data, which in this way makes a wrongful gain or loss to any individual. And at that point of time, such body corporate will be subject to pay damages.[18] However, the major drawback is that it deals with only 'corporate bodies' and it not sufficient enough to cover the entire data dominion.

In present time, due to the outbreak of novel corona virus (hereinafter 'COVID-19'), the government came up with '*Arogya Setu*' App, which provides medical information about other people. Along with this, the issue of privacy also comes into picture. Many people claim that it violates privacy of the

---

[11] Digital Information Security in Healthcare Act 2018, s 28.

[12] Anirudh Burman, 'Will India's Proposed Data Protection Law Protect Privacy and Promote Growth' (*Carnegie India*, 9 March 2020) <https://carnegieindia.org/2020/03/09/will-india-s-proposed-data-protection-law-protect-privacy-and-promote-growth-pub-81217> accessed 3 April 2020.

[13] PRS Legislative Research, 'The Personal Data Protection Bill, 2019' <https://www.prsindia.org/billtrack/personal-data-protection-bill-2019> accessed 3April 2020.

[14] The Personal Data Protection Bill (2019), cl 3(36)(ii).

[15] The Personal Data Protection Bill (2019), cl 17 and 18.

[16] *K.S. Puttaswamy v. Union of India,* (2017) 10 SCC 1.

[17] Anirudh Burman (n 12).

[18] The Information Technology Act 2000, s 43-A.

patient but if we look at the other side, the government is just giving public interest, an upper hand over private interest. As per to the Epidemic Diseases Act, the government can take necessary steps to tackle the spread of the disease,[19] which may include infringing the right of privacy. Moreover, the protection of the personal data bill says that in case of medical emergency, the protection of data may be waived off without the consent of the individual.[20]

At last, we can say that data related to health issues is a matter of great concern, especially the right to privacy, which is enshrined under Article 21 of Indian Constitution. It is high time to implement Digital Information security in Healthcare Act (DISHA) so that the digital health data of a person is completely secure and remains in privacy.

III. INTERNATIONAL BEST PRACTICES AND REFERENCES

A. The United States of America

USA has been following a sectoral approach to data protection legislation so far. At the federal level, currently, USA does not have any formal legislation regulating the collection and use of personal information. In fact, there is no explicit 'right to privacy' enshrined in the US Constitution, but there are certain sectors creating overlapping protections. The following rules which govern health information and privacy, illustrate this problem.

The Health Insurance Portability and Accountability Act 1996 ("HIPAA") **and the Health Information Technology for Economic and Clinical Health Act 2009 ('HITECH')**

HIPPA[21] was introduced as a response to the digitization of data in the U.S. health care industry and the mounting distress concerning the privacy and security of personal health information. HIPPA established national security standards for 'use' of such health information and privacy standards for the 'protection'.[22] After a span of time, in 2009, HITECH was introduced in order to promote the eloquent use of technology facilitating personal health information. It required a 'notice' to be served to the patients and the US Health and Human Services department (hereinafter 'HHS') in case of a breach of an unsecured and protected health information.

---

[19] The Epidemic Disease Act 1897, ss 2 and 2 (a).

[20] The Personal Data Protection Bill, 2019, cl 12.

[21] Health Insurance Portability and Accountability Act of 1996, Pub L No. 104191, 110 Stat 1936 (1996), (codified as amended at 42 USC § 1320 d (2012).

[22] The National Academies, 'Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research' Washington (DC): National Academies Press (US) (2009).

Pursuant to this, the 'Privacy Rule'[23] and 'Security Rule'[24] promulgated by the HHS created certain individual rights and commanding restrictions on use and disclosure of health information. Ultimately, both these rules created a federal floor of health information privacy protection.

HIPAA and HITECH being the primary health privacy and security law in the U.S. are self-contradictory in nature. Both these regulations including the HHS regulations only apply to organizations and entities which fall under the definition of 'covered entity'.[25] A covered entity within the meaning of HHS regulations can be defined[26] as:

(a) A health plan;

(b) A healthcare clearing house; or,

(c) A health care provider capable of transmitting personal health information in electronic form.

This means that the consumers are not even aware about their personal health information. They never know at what point of time their information is secure and when it isn't because of overlapping and contradictory patchwork of existing protections where separate privacy laws govern specific areas of U.S. healthcare system.[27] However, these separate pieces have been instrumental in securing health data and efficient data collection and transfer.

B. Australia: The Privacy Act 1988

In Australia, the Privacy Act,[28] so far as it regulates the Commonwealth public sector and the national private sector, provides extra protection around handling of health information by controlling how the health service providers collect and handle personal health information. Even though, there is no absolute 'right to privacy' in Australia just like the United States, the nation has a comprehensive law dealing with the sectoral regulations of the right to privacy.[29]

---

[23] HIPAA Security and Privacy Regulations 2018, ss 160.101 and 164.104.

[24] General Security and Privacy Provisions 2018, ss 160.103 and 164.306.

[25] Covered Entities and Business Associates, US Department of Health and Humans Services (16 June 2017) <https://perma.cc/4SWX-KLBH> accessed 3 April 2020.

[26] 45 C.F.R. § 160.103 (Defining 'covered entity').

[27] Nuala O'Connor, 'Reforming the US Approach to Data Protection and Privacy' (*Council on Foreign Relations*, 30 January 2018) <https://www.cfr.org/report/reforming-us-approach-data-protection> accessed 3 Apr 2020.

[28] The Privacy Act 1988 <https://www.legislation.gov.au/Series/C2004A03712> accessed 3 April 2020.

[29] Tanvi Mani, 'Privacy in Healthcare: Policy Guide' (*The Centre for Internet & Society*, 26 Aug, 2014) <https://cis-india.org/internet-governance/blog/privacy-in-healthcare-policy-guide>

All health service providers including the ones that merely hold the health information fall within the Privacy Act. The manner, in which health information is collected and handled, is regulated by the Act. Since the act is administered by the Office of the Australian Information Commissioner (hereinafter 'OAIC'), there are regulations within the Act which create a balance between protecting health information from unexpected uses beyond healthcare and advancing public health through medical research.[30] In lieu of this, there are two binding set of guidelines issued by the National Health and Medical Research Council within the meaning of Section 95 and 95A of the Act.[31]

The guidelines refer to:

(a) The procedures that medical researchers must follow in case of disclosure of personal health information from a Commonwealth organization for research purposes.[32]

(b) The framework to assess proposals to handle personal health information held by organizations without the informed consent of individuals.[33]

It is pertinent to note, that the Privacy Act cannot stop a health service provider when informed consent has been obtained from the individual, however, in the absence of such consent, the Act allows disclosure of genetic information in limited instances such as cases where health service needs to be provided to that respective patient.[34] Also, where there is a serious threat to life of a genetic relative of the patient and when the health service provider is in compliance with the guidelines provided under Section 95AA of the Act.[35]

IV. RE-EVALUATING CONSTITUTIONAL PROTECTION FOR HEALTH INFORMATION PRIVACY

These are extraordinary times for a strong and independent India, where a public healthcare disaster has taken the world to a position where almost everybody is becoming submissive and where countries are giving up and losing all hopes. For all that we know, the last time such global panic and terror prevailed was during the World Wars. The discussion on human culpability in light of the COVID-19 outbreak has just started and is probably going to

accessed 3 April 2020.

30 Australian Government, Office of the Australian Information Commissioner <https://www.oaic.gov.au/privacy/the- privacy-act/health-and-medical-research/> accessed 3 April 2020.

31 *Ibid*.

32 The Privacy Act 1988, s 95.

33 The Privacy Act 1988, s 95-A.

34 Tanvi Mani (n 29).

35 The Privacy Act 1988, s 95-AA.

overwhelm global talk and governmental issues for times to come.[36] The main aim of India is to focus on the prevention, mitigation and control of Covid-19. For this purpose, both the Central and the State Governments have taken a number of measures and both of them are working in harmony with each other.

COVID-19 has been declared as a pandemic as it has hit more than 4.4 million people across the world, and has taken over 3,00,000 lives till date. Emerging from China, the novel virus has affected most of the world including the greatest superpower, U.S.A where close to 1.45 million people have been affected and 85,000 people have died. Even in India, the total number of affected people as per official records is around 80,000, with the death toll being over 2,600. Since, no vaccine or effective treatment is available for treatment; most of the countries have adopted the method of lockdown as social distancing has proven to be an effective tool, which can stop the spread from spreading. India is also under lockdown since 25th March 2020 which is recently extended for another two weeks and now it will last till 17th May 2020.

Looking at this current situation, some states in India published an online database of people who have been infected with this disease or are quarantined in their respective homes or in government centers. Some states even went ahead and pasted notice outside the houses of those people who are quarantined probably in good faith that it will alert the other people who are living in the vicinity.

The whole issue of stopping the pandemic by the State through different measures like these will face an obstacle in the form of privacy of the people or at the time of pandemic, the issue of privacy will take a backseat to give way to a larger public interest.

In Justice *K.S. Puttaswamy* v *Union of India*,[37] right to privacy was recognized as an integral part of right to life under Article 21 of the Constitution of India and later on reinforced in *Puttaswamy II*.[38] However, the right to privacy is not an absolute fundamental right like any other fundamental rights under the Constitution of India and therefore, it can be curtailed by the State as per the Constitution. Even in the *Aadhaar* case, three conditions were laid down to test the validity of an Act infringing any right; first activity must be endorsed by law (lawfulness). Second, the activity must be essential for a real

---

[36] Wendy K. Mariner, 'Reconsidering Constitutional Protection for Health Information Privacy' (2016) 18(3) University of Pennsylvania Journal of Constitutional Law 975 <https://scholarship.law.upenn.edu/jcl/vol18/iss3/6> accessed 27 April 2020.

[37] (2017) 10 SCC 1.

[38] Writ Petition (Civil) No 494 of 2012.

point (need). Third, the activity (infringing privacy) must be proportionate to the requirement for such activity.[39]

The judgment in *Puttaswamy II* further stressed on the doctrine of proportionality by articulating four sub-parts:

(a) A measure restricting a right must have a legitimate goal.

(b) It must be a suitable means of furthering this goal.

(c) There must not be any less restrictive but equally effective alternative.

(d) The measure must not have a disproportionate impact on the right holder[40].

Any State, which has published the names and addresses of people who are suffering from COVID 19 and also pasted the so called notice outside the homes of the people who are quarantined seem to be violating the right to privacy of such people. The action of the States will lead to a constitutional question, whether all these measures adopted by the States can withhold the judicial scrutiny as laid down by the Supreme Court in the *Puttaswamy* Case.

Today, as India fights this dangerous pandemic, The Central Government launched the 'Arogya Setu' mobile app to alert users if they are into contact of a COVID-19 positive patient and what kind of precautions can they take in such case. However, the cyber security experts raised this issue that 'Arogya Setu' could violate the right to privacy of a COVID-19 positive patient.[41] As per the privacy policy of the app, it collects the personal data of its users and discloses such health data to the Government with necessary details for 'carrying out medical and administrative interventions necessary concerning COVID-19'.[42]

The app is also more invasive. It collects multiple and personal sensitive data which raises a threat to privacy. However, it is also justifiable to say, that during the outburst of any epidemic disease, the Central Government has the

---

[39] Vikram Koppikar, 'Covid-19: Data Privacy in these Testing Times' (*Money Control:India*, 27 April 2020) <https://www.moneycontrol.com/news/economy/policy/covid-19-data-privacy-in-these-testing-times-5120201.html> accessed 27April 2020.

[40] Soutik Banerjee and others, 'Privacy in Times of Corona: Problems with Publication of Personal Data of COVID-19 Victims' (*Live Law*, 26 March 2020) <https://www.livelaw.in/columns/privacy-in-times-of-corona-154360?infinitescroll=1> accessed 27 April 2020.

[41] Manavi Kapur, 'The Corona Virus App Narendra Modi Endorsed is a Privacy Disaster' (*Quartz India*, 15 April 2020) <https://qz.com/india/1838063/modis-aarogya-setu-coronavirus-app-for-india-a-privacy-disaster/> accessed 27 April 2020.

[42] Kashish Aneja and Nikhil Pratap, 'Implement Arogya Setu but Only through Law' (*The Hindu*, 21 April 2020) <https://www.thehindu.com/opinion/op-ed/implement-aarogya-setu-but-only-through-law/article31391708.ece> accessed 27 April 2020.

power to take all the 'necessary measures' to prevent the spread of such disease for the interest of the public at large.[43]

If at all the right to privacy of a person has to be restrained, it must be through a valid and sanctioned law which should be passed by the legislature. On examining the relevant laws including The Epidemic Diseases Act, 1897, and The National Disaster Management Act, 2005, there appears to be no legal provision which lays out for the personal health data of the consumer to be published in a public database. This preliminary illegality notwithstanding, the State's action also falls foul of the test of 'proportionality'.[44]

Any action of the Central or State government, which violates the Fundamental rights of its citizens, in order to satisfy the test of proportionality, must ensure that it is not 'excessive'. What it means is that, there should not be any existing measures that are equally effective with a lesser degree of encroachment.[45] *Puttaswamy*[46] calls this the 'necessity stage'. The policy followed by some of the Governments has been to use indelible ink to stamp those people who have been tested positive or have been quarantined.

The action of the States may have a reasonable goal, (ie to prevent and control the spread of Covid-19 by minimizing contact of people and following social distancing). Given that the State's main aim is that the people who have been affected by the virus do not come in contact with the other people, it would appear that physical stamping and identification of homes completely achieves the said aim, and the publication of a database of the patients is entirely excessive.

There are a number of problems with the publication of an online database which consists of personal health data of the COVID-19 patients. With no specific Data Protection law in the country which prima facie is a continuous violation of the order of the Supreme Court while upholding the constitutionality of the *Aadhaar Act*,[47] the personal data of these people, without their consent, is being set out in the public domain and is exposed to being misused and abused.

This pandemic has also seen a rise in xenophobia, prejudice and racial violence, and there have been reports of hate crime, mob lynching in that respect.

---

[43] Epidemic Diseases Act 1897.

[44] Soutik Banerjee and others, 'Privacy in Times of Corona: Problems with Publication of Personal Data of COVID-19 Victims' (*Live Law,* 26 March 2020) <https://www.livelaw.in/columns/privacy-in-times-of-corona-154360?infinitescroll=1> accessed 27 April 2020.

[45] V.N. Shukla, *Constitution of India* (11th edn, Eastern Book Company 2008).

[46] Writ Petition (Civil) No 494 of 2012.

[47] *K.S. Puttaswamy* v *Union of India*, (2017) 10 SCC 1.

Along with the infected patients and quarantined people, the doctors and nurses who are the only ones treating Covid-19 patients are reportedly facing hate, abuse, and discrimination. All this is making the patients and their families, a lot more vulnerable.

We are living in the time where once any information is uploaded for public eyes on the internet; it is never capable of being completely removed from there. The personal information of those who are quarantined for Covid-19 will outlast the present virus and will remain in the public domain forever. Then what happens to the rights of these humans to be forgotten on the internet, and what happens with their identification once it is reduced to an entry on a stigmatized database? Stigma, as we recognize from history, tends to a long way to outweigh rationality and sagacity, and has a lifespan of its own.

It is mostly the propensity of States to consider civil liberties as crucial in times of such crisis, war, or emergency. Some people advocate that it is the right thing to do, and arguably, the Constitution recognizes this by providing for art 352-360[48] which envision a very different society in times of emergency. Nonetheless, in dealing with COVID-19, we must acknowledge that civil liberties and rights are not at all the gift of the Executive, and the true test of any democratic Government is to deal this crisis with least possible deviance.

The whole world including India is fighting an invisible enemy in the form of Covid-19. It is not the first time the world is dealing with such a pandemic. There are a number of instances in the past where the World has dealt with many such pandemics e.g. the first reported yellow fever in Yucatan in 1648 to the Ebola Virus and the 2003 SARS outbreak in Toronto. Just like any medical emergency, even in this emergency some of the civil rights are taking a backseat in public interest and like all the viruses in the past, even this virus will also leave us one day or will subsidize to such an extent that we can get back to our normal life but we all need to be guarded against any excessive abuse on our liberties by the executive in this regard.

V. CONCLUSION

Consumer privacy, in the context of healthcare is extremely vital. While India continues to extend its lead in the race towards a culture of privacy, it can also fall for a poor second in no time. The amount of consumer health data collection is increasing exponentially and very little is known about the extent to which this data is being shared with third parties especially when we are dealing with an invisible enemy in the form of COVID-19.

[48] Constitution of India, pt 18.

Some well renowned commentators like Edward Snowden and Yuval Noah Harari have already warned the world that increasing surveillance for tackling the present healthcare crisis can make surveillance state the 'new normal' thereby threatening the privacy of the people. A responsible and democratic state will only collect that much information as it is needed for achieving the specific objectives and once the objectives are achieved shall delete such data. While DISHA and NEHA sound promising enough, their implementation and enforcement chiefly remains untested, not to forget the Personal Data Protection Bill of 2019, which still remains a hesitation.

Implementing DISHA and NEHA as a regulatory response would make India, a front runner in the regulation of healthcare data, in this crucial hour, when governments all around the globe are still scrambling to narrow down a proper definition of 'personal information' in their respective legislations along with the rights and controlling access of such information.

Since India is stepping up to create an overarching legislation on data privacy and security, the timing of both the drafts seem to be questionable. If such a lack of coordination and consistency exists between the ministries, it could lead to irregularities athwart to sectoral regulations of health data and also shift back India in the race towards attaining the much awaited 'culture of privacy'.