DISSERTATION

A CRITICAL ANALYSIS OF THE DNA TECHNOLOGY (USE AND APPLICATION) REGULATION BILL 2019 WITH SPECIAL REFERENCE TO THE RIGHT TO PRIVACY IN CRIMINAL JUSTICE ADMINISTRATION

SUBMITTED TO

INSTITUTE OF LAW, NIRMA UNIVERSITY

AS A PARTIAL FULFILLMENT OF REQUIREMENT FOR THE

DEGREE OF MASTER OF LAWS (LL.M)

UNDER THE GUIDANCE OF

DR. PURVI POKHARIYAL

DEAN AND DIRECTOR

INSTITUTE OF LAW, NIRMA UNIVERSITY

SUBMITTED BY

MEDHA SINGH

19ML015

Table of Contents

DECLARATION

I, Medha Singh, bearing roll no. 19ML015, do hereby declare that the dissertation submitted is original and is the outcome of the independent investigations/ research carried out by me and contains no plagiarism. The dissertation is leading to the discovery of new facts/ techniques/ correlation of scientific facts already known. This work has not been submitted to any other University or body in quest of a degree, diploma or any other kind of academic award.

I do hereby further declare that the text, diagrams or any other material taken from other sources including [but not limited to books, journals and web] have been acknowledged, referred and cited to the best of my knowledge and understanding.

Date:

_____

Name: Medha Singh

Roll no. 19ML015

Course: Criminal Law

Institute of law

Nirma University

CERTIFICATE

This is to certify that the dissertation entitled "A CRITICAL ANALYSIS OF THE DNA TECHNOLOGY (USE AND APPLICATION) REGULATION BILL 2019 WITH SPECIAL REFERENCE TO THE RIGHT TO PRIVACY IN CRIMINAL JUSTICE ADMINISTRATION" has been prepared by Medha Singh under my supervision and guidance. The dissertation is carried out by her after careful research and investigation. The work of the dissertation is of the standard expected of a candidate for Master of Laws [LLM] in Criminal Law and I recommend it be sent for evaluation.

Date:

_____

DR. PURVI POKHARIYAL

DEAN AND DIRECTOR

INSTITUTE OF LAW, NIRMA UNIVERSITY

AHMEDABAD

ACKNOWLEDGMENT

I would like to express my sincere gratitude to my supervisor Prof. Dr. Purvi Pokhariyal, Dean and Director, ILNU, for her continuous guidance, support and supervision for the completion of my thesis. I would like to thank her for her patience and knowledge that has helped me greatly to address this topic and do justice to it to the best of my ability.

Besides my supervisor, I would like to express my sincere gratitude to Dr. Madhuri Parikh, Associate Professor ILNU, my course coordinator and a constant source of support who taught us the basics of research patiently and have made writing this dissertation possible.

I would also like to sincerely thank my institute, Institute of Law, Nirma University, for it would have been very difficult to write a thesis at home during a pandemic, for making it possible and absolutely seamless and providing us with all the resources to complete our research through its library and online databases.

I would like to extend my thank you to Ms. Trisha Mittal, Assistant Professor, Maharashtra National Law University, Nagpur for her suggestion to research on this topic and to help me navigate criminal law with enthusiasm.

And lastly, I would like to extend my gratitude to my best friend, Deepa Dubey, 19ML007, LLM, ILNU, for it wouldn't have been possible to finish this dissertation without her constant aid, advice and discipline.

TABLE OF CASES

17.	Suresh Kumar Koushal v. Naz Foundation and Ors. AIR 2014SC 563,
19.	ADM Jabalpur v. Shivakant Shukla
20.	T. Sareetha v. Venkatasubbaiah AIR 1983 AP 356
21.	A.K. Gopalan v. State of Madras, 1950 AIR 27
22.	Maneka Gandhi v. Union of India 1978 AIR 597

LIST OF ABBREVIATION

- AIR- All India Reporter
- Anr. – Another
- CrPc- Code of Criminal Procedure
- CJA-Criminal Justice Administration
- CJPA- Criminal Justice Police Act
- DNA- De-oxyribo Nucleic Acid
- DPA- Data Protection Authority
- FIR- First Information Report
- Govt.- Government
- IEA – Indian Evidence Act
- IPC – India Penal Code
- MCOCA- Maharashtra Control of Organised Crime Act
- NCRB – National Crime Record Bureau
- PIL- Public Interest Litigation
- SCC- Supreme Court Cases
- UK- United Kingdom
- UN- United Nation
- UOI – Union of India
- USA- United States of America
- v. – Versus

CHAPTER 1

INTRODUCTION

1.1 INTRODUCTION

Primary evidence is one of the pillars of the Criminal Justice Administration upon which the conviction and acquittal can solely depend. If this primary evidence is in the form of a bodily fluid, hair, fingerprint, nail, saliva etc. it can ascertain the culpability beyond a reasonable doubt. Hence it is pertinent to mention that our constitution provides a safeguard to the accused in the manner of fundamental rights. An accused can chose to not answer any incriminating questions and any method of compulsion violates his right. This "right" found its nexus in the ever-growing ever-evolving Right to life and personal liberty. These seem interlinked and intertwined and very believably they are so. The right of privacy has very recently received popularity with the advent of the judicial pronouncement from the case of *K. S. Puttaswamy*[1] which declared that the right to privacy is protected as part of the right the life and personal liberty under the Constitution of India. Historical evidence dating back five decades show that the Supreme Court has been approached many times for the determination of the right to privacy in criminal cases ranging from *M. P. Sharma v. Satish Chandra*[2], *Kharak Singh v State of UP*[3], *Govind v. State of M.P*[4]., *PUCL v UOI*[5] before the 9 judge bench infamous *Privacy case* took cognizance of the matter. Overruling the *Aadhar judgment* the *Privacy case* ended the

[1] Infra n. 8, p. 13
[2] Infra n.18, p. 23
[3] Infra n.19, p. 24
[4] Infra n.26, p.26
[5] Infra n.34, p.28

debate over matters concerning privacy by a unanimous verdict of the entire bench. The judgment has provided for the grounds of the right to privacy and the limitations on state action, but what the critical detailed analysis reveals is that it has so much more to offer. The decision embarks the readers on a journey that begins from the tussle between the individual's liberty and the state. There are needless to say lacunas in the judgment that it has remiss on a few points of important decisional matters. This judgment also laid down several guidelines that should have been kept in mind so all the laws that follow this judgment and have any bearing on the matters of privacy should be in consonance to the guidelines laid down in this judgment. However, the present Union Govt. irrespective had initiated the DNA Technology (Use and Application) Regulation Bill 2019[6], reviving it from 1984. The *Puttaswamy* judgment recognizes multiple facets of the right to privacy and within it the right to preserve "personal information". It recognizes "personal information" as "data" that should be protected by the State and not misused as means of state surveillance. With this affirmation of data, DNA is genetic data, as per the Section 2(19) of the Personal Data Protection Bill 2019[7] and another in 2019, which is the new initiative by State to strengthen the already existing data protection regime.

A bare reading of the provisions of this bill will only give the idea as to why DNA should be used and what for. But the Bill is very vague in its wording and does not afford and importance and recognition to the fact that DNA is "Data" and there can't be a DNA Bill without the preceding Data Protection Bill. The proposition of the DNA Technology (Use and Application) Bill 2019 is an initiative focusing primarily on DNA data.

[6] The DNA Technology (Use and Application) Regulation Bill. 2019, Bill No. 142-c of 2018, As passed by Lok Sabha on 08.01.2019

[7] The Personal Data Protection Bill, 2019, Bill No. 373 of 2019, As introduced in Lok Sabha

The Chapters proceed with the critical analysis of the DNA Bill, the appraisal and critique of the *Puttaswamy* judgment which encompasses the jurisprudential journey of the Judiciary to arrive at this judgment addressing liberty, dignity and their interrelations with privacy, followed by the International perspective on privacy and genetics law followed by the analysis and suggestive model of for the Personal Data protection Bill.

1.2 STATEMENT OF PROBLEM

The legislature's objective of the DNA bill as per its preamble states only that DNA shall be used, to determine identity and has categorized the stakeholders in the following- victims, offenders, suspects, missing persons, under trials and unknown deceased persons. At the bare reading of the provisions, the Bill seems restrictive in its preamble and does not adequately address every issue pertaining to the use of DNA. The Bill does not elaborate furthermore on the kind of DNA, the specific use, disposal etc. and is remiss on the point of protection of privacy. The biggest red flag of all is that it vests the final overriding powers with the state and its agencies with matters regarding the Regulatory Board and DNA data banks which can be inferred as a conflict of interest and state surveillance. The DNA Bill and the Data Protection Bill need to be analyzed thoroughly from a substantial point of view to determine whether they align their objectives according to the privacy safeguards as held in *Puttaswamy*.

1.3 LITERATURE REVIEW

1) GAUTAM BHATIA, **PRIVACY AND THE CRIMINAL PROCESS: SELVI V STATE OF KARNATAKA,** The Transformative Constitution- A Radical Biography in Nine Acts

This Article in this book is the inspiration for this paper. It has very precisely and accurately given the accounts of the cases that led to the privacy judgment. It discussed in great detail about the right of self incrimination under the right to life and liberty.

2) SAHRDC, **THE FERREIRA CASE: ALL THAT IS WRONG WITH TORTURE AND NARCO-ANALYSIS**

This paper discusses in detail the Arun Ferreira case that highlighted the use of narco-analysis and "Truth Serum" to exact confessions out of accused persons. This article is written in the backdrop of the Selvi Judgment and says that the uses of these techniques of interrogation are not only against self-incrimination but also against one's basic human right against torture.

3) DHIRAJ R DURAISWAMI, **PRIVACY AND DATA PROTECTION IN INDIA**

This article provides an overview of the data protection laws in India before the proposal of this bill and how it has affected privacy, the enforcement and liability provisions of those laws, and pending regulations and trends to protect privacy and enhance data governance practices.

4) MADISON JULIA LEVINE, **BIOMETRIC IDENTIFICATION IN INDIA VERSUS THE RIGHT TO PRIVACY: CORE CONSTITUTIONAL FEATURES, DEFINING CITIZENS' INTERESTS, AND THE IMPLICATIONS OF BIOMETRIC IDENTIFICATION IN THE UNITED STATES**

This paper discussed that following the Supreme Court of India's declaration that privacy is a fundamental right, the idea of a general-purpose identification database is

constitutionally questionable. There is no comprehensive legal framework for privacy protection and no explicit constitutional right to privacy in India. It also criticizes the Aadhar system and renders is against the provisions of constitution.

5) VEENA NAIR, **REVIEW OF THE EVIDENTIARY VALUE OF DNA EVIDENCE**

This paper talks about the kind of evidence in the current technologically advanced time and what it this advent of technology means for DNA evidence. It also discusses the various judicial pronouncements by the Supreme Court in relation to DNA evidence.

6) GAUTAM BHATIA, **STATE SURVEILLANCE AND THE RIGHT TO PRIVACY IN INDIA: A CONSTITUTIONAL BIOGRAPHY**

This article presents an analytical and chronological history of the Indian Supreme Court's engagement with the right to privacy. This article gives a comprehensive, doctrinal understanding of the constitutional right to privacy, as evolved, understood and implemented by the judiciary.

7) NIMISHA SRINIVAS and ARPITA BISWAS, **PROTECTING PATIENT INFORMATION IN INDIA: DATA PRIVACY LAW AND ITS CHALLENGES**

This paper presents an overview of various data protection regimes, followed by an analysis of the Indian position on data privacy.

8) NATALIE A. BENNETT, **A PRIVACY REVIEW OF DNA DATABASES**

This paper is brilliantly written and offers great insight in the DNA Privacy in the United States. This paper has beautifully critiqued the DNA Databases and is very helpful in the analysis of the provisions of the same in the DNA bill 2019 in India.

9) ANIRUDH BURMAN, **WILL INDIA'S PROPOSED DATA PROTECTION LAW PROTECT PRIVACY AND PROMOTE GROWTH? THE GROWTH OF PRIVACY AND THE BILL**

This is a 45 page detailed report written by the author on the existing legal framework for data protection in India to analyze the innovation and determine the usefulness of the Bill. The paper argues that the bill does not address the privacy related harms in the data economy in India. The paper addresses the important of securing informational privacy in great detail.

10) STUDENT ADVOCATE COMMITTEE, **TRANSCRIPT OF THE VII ANNUAL NATIONAL LAW SCHOOL OF INDIA REVIEW SYMPOSIUM: BRIDGING THE SECURITY-LIBERTY DIVIDE**

This piece of document is the summarized written version of the symposium on the aforementioned topic. The most important session of this symposium is the Session I- *Securing Liberty from the State- Redefining Criminal Thresholds in Law.* Wherein many eminent jurists and speakers shared their views and concerns over the national interest that lies in safeguarding privacy as well as ensuring that the rule of law is upheld. Some of the eminent speakers in the panel were Justice Bilal Nazki of the Jammu and Kashmir High Court, Mr. Bharat Karnad, Mr. Yug Mohit Chaudhary, Mr. Shivam Divan, Mr. Gautam Bhatia. The Session II- was on *Intrusive Intelligence - Surveillance Programs and Privacy in India.* During this session some very important points were made regarding the

AADHAR judgment and its subsequent implications. The role of the police was also discussed in the session. The Session III*: Beyond Borders: Extradition, Asylum And Concerns Of State Security* talked about the international perspective on the privacy and data protection regime and gave the right to privacy a human rights hue.

11) THOMAS P CROCKER, **FROM PRIVACY TO LIBERTY: THE FOURTH AMENDMENT AFTER LAWRENCE**

This 71 page research paper is authored on the premise of the landmark judgment of *Lawrence v. Texas*, and how the government in the United States is entitled to access information of individuals subject to the fourth amendment. This paper has proven important to understand what the IV amendment was all about and why did the judiciary in our country chose to not incorporate the provisions of this amendment in our constitution in the case of *M.P. Sharma v. Satish Chandra.*

12) CHRISTINA M. GAGNIER, **ON PRIVACY: LIBERTY IN THE DIGITAL REVOLUTION**

This paper is written by the author after the detailed study of John Stuart Mill's contributions on Liberty. She goes on to explain how United States as a very developed and progressive state, both technologically and otherwise struggles to recognize the private spheres where liberty and privacy are intertwined. This paper critiques that the United States jurisprudence only recognizes the right to privacy in very limited spheres. This paper also gives a peek into the right to privacy of those whose lives revolve in the public eye and once their careers are in public domain, the legitimate concern of privacy is diluted.

13) WARERENR. WEBSTER JR., **DNA DATABASE STATUTES AND PRIVACY IN THE INFORMATION AGE**

This paper talks about how the advent of DNA technology has led to many constitutional concerns all around the world, ever since it became an accepted piece of evidence. The author goes on to explain that the US Federal and State government are unaware of the problems that surround the DNA Databases. Although, in the US they have a CODIS Combined DNA Identification System and Sex offenders Registration which proves very effective in criminal investigations, yet there are still confidentiality and privacy related issues. This paper has proven very useful in evaluating the DNA BILL and whether the prescribes provisions in the act will adequately protect the privacy of the individuals whose DNA will be in this said database.

14) VIKRAM IYENGAR, **MARYLAND V. KING: THE CASE FOR UNIFORM, NATIONWIDE DNA COLLECTION AND DNA DATABASE IN THE UNITED STATES**

This paper talks in detail about the landmark judgment of United States Supreme Court in *Maryland v. King*, in which the it was held that the government after following legitimate procedures under the IV Amendment, after making an arrest on probable cause has to enter that person's DNA into DNA Databases, which was a celebrated decision at the time, although the Coram that gave this decision also warned that this is letting too much power in the hands of the State to have control over a person's DNA and appropriate it on their whims and fancy. This paper critiques the dissenting opinion held in this case, and this paper has proven to be the Contemporary comparison to the case of *Selvi v. State of Karnataka* in India.

15) SHELDON KRIMSKY AND TANIA SIMONCELLI, **GENETIC JUSTICE-DNA DATA BANKS, CRIMINAL INVESTIGATIONS AND CIVIL LIBERITES**

This book has proven very useful to do comparative analysis of the DNA databases in various other jurisdictions. It goes into great detail about the kinds of criminal legal systems in various common as well as civil law countries. It has proven very effective in drawing a contrast and for chalking inferences for changes that can be incorporated in our legal system.

1.4 CONCEPTUAL CONTEXT

1. DNA DATA

Every person has a unique genetic code that we call their DNA that distinctly distinguishes them from others and it is the indication of a person's hereditary information and an explanation of his physical appearance. Every shred of a person is his DNA. For the sake of simplistic understanding, the chemical structure of DNA for the purposes of evidence and such is same as a human fingerprint. But it is not a perfect explanation as DNA is much more complex and is more information rich. Recovering DNA of an alleged accused at a crime scene, after forensic examination shall not only reveal his identity but will also provide with his ancestry and hereditary information etc. that will in-directly end up incriminating his family and kin sharing the same DNA and will ultimately lead to an invasion in their privacy as well. The workability of DNA as evidence in investigation is towing the lines of privacy and self-incrimination. Hence considering DNA as data or Genetic Data should be afforded protection under the Personal Data Protection Bill before the DNA Databases are constituted.

2. DNA PRIVACY AND EXISTING LEGISLATION

The Bill in question is poorly drafted and can be called vague at best. The potential pitfalls of the databases as mentioned in this bill are a threat to the bodily integrity of the citizens who are the kin of the person who's DNA has been collected and are subjected to non-consensual sampling of their genetic material. It is also the violation of their privacy rights as their DNA can be used in the future for fabricating evidence and false accusations. The prospect of long term bio-surveillance occasioned by the storage of genetic information in these DNA databases are opening prospects for illegal use of these collected DNA. The bill does not speak of any of this concern. There is only the wide interpretations by the advent of judgments by the Apex Court that offer some kind of protection to the personal privacy of an individual.

3. PERSONAL DATA PROTECTION BILL

The Personal Data Protection Bill that defines genetic data as a matter of personal information to be protected is a step in the right direction. Under section 2 sub-section (20) it states - **"Genetic data"** means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the behavioral characteristics, physiology or the health of that natural person and which result in particular, from an analysis of a biological sample from the natural person in question; and also defines under section 2 sub-section (21)- "**Harm"** which shall include -bodily or mental injury, loss, distortion or theft of identity, any discriminatory treatment, loss of reputation, or humiliation, any subjection to blackmail or extortion, any observation or surveillance that is not reasonably expected by the data principal. It can be construed from the reading of these tentative provisions that this bill seeks to protect genetic data and any

harm that shall befall in the prospective event that this data is misused. Having stated that, the logical inference drawn is that the Personal Data Protection Bill is advertently better drafted than the DNA Bill and must precede it.

4. DECISIONAL AUTONOMY and INTIMATE DECISON

The basic concept of decisional autonomy stems from the liberty of the individual and the liberty of the individual will comprise of two things the choices and the spaces of the body and the mind. The "inviolability and worth of a human body" is what will give him the liberty of choice and that choice shall always be free and without the interference of state or state actors. Decisional Autonomy restricts the intervention of anyone from making the choices that are intimate to a person's life. This is why privacy cannot exist without having the unwarranted freedom from being coerced into wanting something else for example the guaranteed freedoms in Part III of our constitution such as the Freedom of Religion, freedom to move freely and inhabit any place, the freedom of sexual orientation, freedom to marry etc. The concern of privacy with reference to intimate decision and decisional autonomy goes beyond the mere physical aspects of a persons' individuality but also his creativity, his attributes and the choices he makes in his institutions such as marriage, family, etc. and this cannot be achieved if there is a constant looming threat of state surveillance.

5. PRIVATE REALM

The private realm is the spatial control of an individual. This comprises the institutions he is a part of and also the privacy of his mind to have the freedom of choices. Private realm is a person's sanctuary, his repose and his safe haven where he is uninterrupted from outside influence. Bentham introduced the *Theory of Panopticon* wherein he states that a

person (in his example, a prisoner) will never be certain if he's being watched or not. Meaning that power and the exercise of that power should be visible and not in secret leaving the person in a constant state of angst. Hence the private realm is the place where an individual is free from state surveillance.

6. INFORMATIONAL SELF-DETERMINATION

Informational self-determination is strictly restricted to a person's mind and the information that he stores in it voluntarily or otherwise. Informational self-determination means that when a person has been afforded the right to privacy that shall also afford him control over all the information that's personal to him and also the dissemination of that information. For example, the narco-analysis and brain mapping techniques of extracting confessions are frowned upon for this reason only. The informational self-determination is also crucial to the personal data protection and the recognition of a person's right to control the disclosure and if need be the right to be forgotten from the web of information.

1.5 AIM OF THE STUDY

- To study the wide connotation of privacy of the individual and the limitations of the State with respect to Article 21.
- To analyze in detail the meaning of the right to privacy in respect of DNA evidence.
- To critically analyze the Personal Data Protection Bill 2019.
- To critically analyze the DNA Technology (Use and Application) Bill 2019.

1.6 SIGNIFICANCE OF THE STUDY

The significance of this study is that it shall provide for a compelling argument for the enactment of the Data Protection Bill and against the DNA Bill.

1.7 SCOPE OF THE STUDY

The scope of the study shall be limited to the Supreme Court judgments on the Right to privacy, provisions of the Personal Data Protection Bill 2018 as well as 2019 and provisions of the DNA Bill 2019.

1.8 RESEARCH QUESTION

1. Does the DNA Technology (Use and Application) Bill 2019 adequately address concerns of privacy violations?
2. Why the Personal Data Protection Bill should precede the DNA Technology (Use and Application) Bill?
3. Does the DNA Technology (Use and Application) Bill 2019 adequately address the use of the DNA data by the state?
4. How do the provisions of the DNA Technology (Use and Application) Bill 2019 empower the State to misappropriate DNA data of individuals?

1.9 HYPOTHESIS

The DNA Technology (Use and Application) Bill 2019 is violative of the right to privacy under the veil of compelling state interest.

1.10 RESEARCH METHODOLOGY

The research methodology adopted in this paper shall be doctrinal research. The nature of the study that the researcher undertook involves a critical analysis of the existing literature and suggestions of preventing the drawbacks of the same.

The primary sources of data shall include the data collected from the various existing statues and legislations. It shall include the available data on the official government platforms

The secondary data shall include the journal articles, books and reports.

1.11 CHAPTERISATION

- Chapter I Introduction

This chapter shall deal with the introduction of the research problem, followed by a brief outline of the succeeding chapters. This chapter will also comprise of the hypothesis, research questions, literature review, conceptual context, aim and scope of the study.

- Chapter II DNA Technology (Use and Application) Bill- An Analysis

This chapter shall deal with the detailed critical analysis of the provisions of this bill.

- Chapter III The Privacy judgment and the Supreme Court's Interpretation of the Right to Privacy

This chapter shall deal with the interpretation of "right to privacy" through the perspective of individual liberty, autonomy and the tussle between Individual and State.

- Chapter IV International Perspective on DNA Privacy

This chapter shall deal with the existing legislations in the USA, Germany, Australia, Japan and UK on DNA and Genetic Privacy and shall find the congruent provisions that can be applied to our domestic laws.

- Chapter V Analyzing Data privacy- The Data Protection Bill 2019

This chapter shall deal with the detailed appraisal and critique of the Data Protection bill and its merits and demerits.

- Chapter VI Conclusion and Suggestion

This chapter shall include concluding remarks and a suggestive model suitable for India for DNA privacy.

CHAPTER 2

CHAPTER II- THE DNA TECHNOLOGY (USE AND APPLICATION) REGULATION BILL 2019- An Analysis

2.1 Historical Background Leading to this Bill

It was the year 1985 when DNA as evidence was accepted for the first time in India, but it was not until this Bill was drafted that and initiative had risen to regulate the use of DNA technology for criminal investigation. Before this Bill there had been several initiatives were taken to draft legislations that incorporated the use of DNA technology. The Department of Biotechnology set up a DNA Profiling Advisory Committee in 2006 which then morphed into the Human DNA Profiling Bill the next year. This draft bill was to include DNA fingerprinting and diagnostics too but it never saw the light of day in the Parliament because it was criticized on the grounds that it did not address privacy concerns, which as it happens, still is an issue at large. In 2013, the Department of Biotechnology set up another expert committee to reiterate on the drawbacks of the 2007 draft bill and to finalize the text of the bill.

Two years later, the government planned to table this bill again in the lower house but due to increasing activism on data protection and the on-going *Puttaswamy*[8] case put a hault on it. Subsequently in 2016, the Use and Regulation of DNA based technology in Civil and Criminal Proceedings, Identification of Missing Persons and Human Remains Bill was listed for introduction, consideration and passing but was met with the same fate as the draft bill in 2015.

The critiques and activists raised same questions of how the bill infringes the privacy of the persons who'd be subjected to this bill be it under-trials, accused persons etc. There were also concerns about maintaining the credibility of the data collected and how it is

[8]Justice K. S. Puttaswamy (Retired) and another v. Union of India and others, 2017(14)SC ALE375

stored, the safeguard for elimination of contamination, theft and possible corrosion of the sample to name a few.

In 2018, the Law Commission of India in its 271st report drafted the bill titled DNA Based Technology (Use and Regulation) Bill 2017, but it was also criticized time and again by the overarching privacy concerns and wonderfully so this bill was drafted a month before the *Puttaswamy* judgment came to be. Since then nothing has been changed in this bill and neither in the 2019 bill to accommodate the privacy guidelines as per the said judgment. [9]

2.2 Critique of the Bill

The DNA Technology (Use and Application) Regulation Bill 2019 aims at using the DNA technology in establishing the identity of a person. And that's about it, at a preliminary glance. In depth reading differs from the preamble of the bill. Chapters VI and VII of the Bill deal with "protection of information" and "offences and penalties" respectively. Under the head of chapter VI, Sections 32 to 38 incorporates provisions to ensure the protection of the DNA samples and profiles. These sections although seek to protect information but are highly inadequate in affording this protection as the wordings of these provisions only impose a suggestive duty rather than a procedure as to how it shall be done. Section 32 and 33 talk only of what is expected out of the authorities dealing in these samples and fails to lay down specific guidelines for the protection of information. [10]

[9], Dr. Shashi Tharoor, Dr. Shashi Tharoor on The DNA Technology (Use and Application) Regulation Bill, 2018**,** available at - https://www.youtube.com/watch?v=ifO2nlY_2QY **,** on 06/07/2020 10:59 pm

[10] Ashima Sharma and Nidhi Pratap Singh, DNA Technology Regulation Bill, 2019 and its Impact on Marginalised Communities, The Criminal Law Blog, National Law University, Jodhpur, 09/07/2020, 11:19 pm, https://criminallawstudiesnluj.wordpress.com/2020/04/01/the-dna-technology-regulation-bill-2019-and-its-impact-on-marginalised-communities/

Under Section 34, is where we find the "alternate" purpose of this Bill that is absent from its preamble. This section states that the DNA profiles, DNA samples and all information relating to them shall be readily available for *other* purposes such as –

- Admission of evidence at trial
- Facilitating criminal investigations by identification and providing evidence to the prosecution
- And any other purpose as may be prescribed by the regulations

These purposes that are crucial to the safety and privacy of an individual's personal information are not highlighted as the objective of the bill but is clearly within the ambit of the "use" of the DNA samples. There is ambiguity as to how these aforementioned purposes shall be carried out and whether there exists a safety net for the individual who's DNA is being used. Sub-section (f) of Section 34 gives a wide power to the State to justify any purpose of the use of the DNA.

Sections 35 to 37 discuss the Access of information that is stored in various indexes and DNA Data Banks. Synonymous to the wordings of the previous sections, these sections also impose duty on the people that the Director deems appropriate to have access to information, which is contradictory since it is the Director of the Regulatory Board who is also the in charge of the DNA Data Banks.

Chapter VIII of the Bill titled "Offences and Penalties" penalizes unauthorized use of the DNA samples. Under Section 45, any person either an employee of the DNA Data bank or otherwise has in his possession the DNA sample and profile of a person who's information was to be secured by the DNA Data bank shall be liable to imprisonment for three years or with 1 lakh rupees fine or both. Section 45 penalizes the unauthorized obtaining of DNA

information by any other person not mentioned in section 46 and similarly any person, who "uses" this unauthorized DNA sample which is obtained under section 47, shall face the same penalty as in section 45.

These sections under Chapter VIII give the penalties of the nature of "contravention of the provisions of this act". They do not prescribe how these shall be prevented in the first place.

This 2019 Bill is laughing stock in the context that it is so insufficient. This bill is not novelty, as has already been aforementioned, and is an attempt by the state to affirm its power over the citizens in the name of public interest. The bill fails to mention what exact information would be extracted to generate a DNA profile of an individual, meaning that there is no limitation on what part of a person's DNA would be used in what situation depending upon for what purpose it is extracted has not been discussed in the bill. For the sake of brevity, for the identification of missing or deceased persons, only parts of DNA need to be matched with and when there is a crime scene investigation where on forensic analysis it is revealed that there are multiple samples of multiple individuals and there needs to be a comparison between two or more, the Bill is silent. This will make a large population of people susceptible to profiling based on the matching characteristics of their DNA with the ones found in an investigation. And to everyone's horror these DNA profiles can be misused for surveillance or even by private entities to pursue blackmailing and for perpetrating crimes by planting DNA evidence to falsely accuse someone. The preamble of this bill also lays down to create DNA profiles for determining pedigree of an individual, his immigration and emigration status, which is a blatant abuse of power and infringement of privacy in the highest manner.

The whole idea behind the objection of the AADHAAR scheme by the government was that it was creating an imbalanced power regime between the State and the citizens. Justice Chandrachud in the *Puttaswamy*[11] judgment says that liberty is in having the freedom of choice, and choice means a choice of preferences, in the privacy of mind. This is to establish that the State already dictates a lot of our lives and our choices, there needs to be a bar somewhere where "we the people" draw the line at State surveillance, if not on everything then in the least our own body and mind.

The DNA Bill's objective lays down that it seeks to identify five categories of persons namely, missing persons, victims, offenders, under trials and unknown deceased persons. It goes on to say in its preamble that the use of DNA technology will only be restricted to the offences mentioned in the Schedule of the Bill which include all the offences under IPC and for some civil matters such as parentage disputes. It then goes on to explain how the collection of the DNA will take place and what shall be the procedure that will be employed in DNA profiling.

One of the most flawed observations in this bill is that it is silent on "effective consent". This bills walks on such shaky grounds, that it doesn't even define the meaning and ambit of the term "consent". By leaving the term "consent" undefined, it opens grounds for uninformed and unambiguous consent.

It says that the bodily substances would be collected by investigating authorities with prior informed consent. For arrested persons, the written consent has to obtained if the person has been accused of an offence is punishable with up to seven years imprisonment. On the

[11] Supra note 1, p. 13 [169]

other hand if the punishment for the offence exceeds seven years imprisonment or to death, then consent is immaterial. Further, if the person is a victim, or relative of a missing person, or a minor or disabled person, the authorities are required to obtain the written consent of such victim, or relative, or parent or guardian of the minor or disabled person. If consent is not given in these cases, the authorities can approach a Magistrate who may order the taking of bodily substances of such persons.

This aforementioned provision under Section 21 and 22 of the Bill, it substantially waters down the real essence of consent by allowing the Magistrate to override the refusal of consent by any arrested person or a refusal of a guardian on behalf of a minor. There are no guiding factors mentioned in this bill to either limit or prescribe the extent of jurisdiction of powers of the Magistrate.

It fails to mention the rights of person in cases of revocation and deletion of their DNA profiles and does not mention the rights of the individuals who had voluntarily submitted themselves to DNA profiling under Section 22 of the Bill. Also, the bill does not provide for provision for informing individuals about the details of the collection and usage of his or her DNA. The bill even goes on to say that it will indefinitely hold the DNA in the DNA data banks of the people who are the victims of the crime. It is important to highlight here that missing persons, if a person is presumed dead for a period of more than seven years, the law presumes him/her dead.[12] So it is obviously contrary to the objective of keeping a "legally dead" person's DNA indefinitely, unless the State has other ulterior motives in mind to appropriate the DNA for incriminating his relatives which is to state the obvious

[12] Section 108 Indian Evidence Act 1872, Section 13 (1) (vii) Hindu Marriage Act 1956

but does make one wonder why'd the state want an over looming power of a person's most private piece of existence. After the *Puttaswamy*[13] judgment the Bill should have given the right to individuals to retain back their DNA from the State after its purpose is fulfilled.

Meaning that wherever you go, whatever you do, from coughing on the side of the road to getting a haircut, if you leave traces of your DNA, the State shall appropriate it and not even inform you. There is absolutely no directions or guidelines that either define or curb the powers of the DNA data banks and laboratories. The few safeguards that the Bill does mention are on the DNA collected from the "body of the person". If the DNA collected from otherwise like scene of the crime, clothing, other sources, the DNA labs can store it without informing the person that their DNA has been collected by an authority of the State, which gives them a very large quantum of DNA. In the absence of a prohibition to store the DNA and on the obligation to destroy the DNA, the DNA laboratories can create their own data banks with no supervision from the government or any government oversight.

Section 31 sub-section (3) of the Bill mentions that persons who is neither an offender nor a suspect or an undertrial, but whose DNA profile is entered in the crime scene index or missing persons' index of the DNA Data Bank, for removal of his DNA profile there from, remove the DNA profile of such person from DNA Data Bank under intimation to the person concerned, in such manner as may be specified by regulations. In other words, innocent persons, who is unaware that his DNA is stored in DNA Data bank need to put in a written request to get his DNA removed from the Data bank or else it would stay there

[13] Supra n.1 p.1

for eternity. This is an impossible burden that the bill imposes on the people while letting the DNA Labs misuse the DNA of innocent persons, hence again establishing, a blatant infringement of the right to privacy, probably in the widest possible sense.

After the Supreme Court's judgment in affirming the right to privacy it has become very apparent that privacy safeguards need to be checked before this legislation is passed. The Bill under Chapters II, III and V, talks about setting up of National and Regional DNA Data Banks for every state or two or more states, setting up DNA Regulatory Board to ensure compliance to privacy safeguard standards. Which seems like a step in the right direction, but it most certainly is not. Ironically, the members or the chairs of these regulatory boards and data banks are the investigating officers, heads of investigating agencies and heads of the DNA labs against whom the safeguard needs to be there, to keep a check on them, hence creating a conflict of interest in the way that the regulators will be regulating themselves. Instead of comprising the Regulatory board with outside experts, forensic scientists, scholars in the field of DNA Technology etc, the Bill empowers the targets of these regulations the right to regulate themselves.

Now that the provisions have been under scrutiny, the practical difficulties need to be addressed too, such as; forensic evidence is fragile and very susceptible to contamination. Henceforth it was not held to be a reliable piece of evidence early on. But one major concern that the bill doesn't address is that the DNA samples of the investigating officer or agency could easily be mixed up or mistaken for that of the accused or suspect, and there's no safeguard to prevent this in the bill. This could be rectified by having an "elimination index" wherein all the officers investigating submit their samples for the process of ruling them out during the course of the determination of the guilt of the

accused, although there isn't an index in the Bill nor does it speak of anything of the sort. The bill mentions 5 categories of persons it seeks to identify using the DNA technology and creates an index for the suspects, under-trials and offenders of whom they can get DNA samples without their consent which is a whole other can of worms that violate personal information.[14]

This also raises more important concerns which may crop up during the indictment of accused on trial. There is absolutely no mention of any sort of obligatory function of the law enforcement agencies during the course of the DNA sample collection. The DNA samples are such important, delicate and volatile piece of evidence that there needs to be an effective mechanism in place to ensure a trusted chain of custody of DNA samples, their reliable analysis, proper use of these samples with a method of expert evidence. These samples will prove very important in the final process of judicial pronouncements and in the absence of these safeguards, there will be perpetrating the criminal justice system. [15]

The DNA Bill's objectives in the preamble also mentions that State shall link the DNA profiles to Aadhar Database only goes further to affirm that this Bill is more harm than good. The way the clauses are open-ended in their drafting, the absence of procedural safeguards gives a very wide powers vested in the instrumentalities of the State proves that this fails to abide by the guidelines of the privacy enunciated by the Supreme Court.[16] To say the least- Privacy should be maintained robustly otherwise Biological Data Breaching can lead to gargantuan atrocities to the mankind.

[14] Supra n.2 p.2
[15] Ibid.
[16] Ibid.

CHAPTER 3

THE PRIVACY JUDGMENT AND THE SUPREME COURT'S INTERPRETATION OF THE RIGHT TO PRIVACY

3.1 Pre-Puttaswamy Judgments- Mapping the Trajectory of Right to Privacy

This part of chapter shall trace the judiciary's rendezvous with privacy. The Apex Court has been approached to, to shed their wisdom on this issue for nearly five decades. The

term privacy isn't mentioned in the Constitution and the Constitution makes no specific reference to it. It wasn't even in the intentions of Constituent Assembly Debates to accommodate something on the line of the American Constitution's IVth Amendment (which prohibits unreasonable search and seizure). Therefore this right had to evolved, dug out from the text of the Constitution and that has been done through the following judgments.[17]

The first case in line was *M.P. Sharma v. Satish Chandra*[18] in 1954 in which the Court held search and seizures as valid. The court gave the reason that this is an example of the State exercising its powers to ensure security and hence it is a valid law. They did not want to restrict this power of the state solely on the basis of this right that didn't even expressly exist in the constitution and did not want an analogy drawn with the American Constitution.

Next case in line was *Kharak Singh v. State of U.P*[19] wherein the UP Police Regulations were questioned on the ground that "history sheeters" (repeat suspects who have been arrested but never convicted) were under police surveillance. This surveillance included domiciliary visits at night, tailing their movements, secret searches of their houses and staking out their homes and frequent places of visit. This surveillance was challenged in the court on the ground that it violated the freedom of movement Article 19(1)(d) and the personal liberty of the individual under Article 21. The Court held these Regulations as administrative exercise of the duties of the state and did not fall under the meaning of law

[17] Gautam Bhatia, "State Surveillance and the Right to Privacy in India: A Constitutional Biography" 26 (2014): 32.
[18] M.P. Sharma v. Satish Chandra, AIR 1954 SC 300
[19] Kharak Singh v. State of U.P.,AIR 1963 SC 1295

and the defense of *"procedure established by law"* under Article 21 falls insufficient here. Hence it was difficult to purport that this Regulation violated Part III. Another important observation in this case from the side of the State was that this exercise of surveillance was in the interest of "public interest" which made it lawful to continue it.

The State inferred and the Court agreed that this surveillance was not routine and was *"targeted"* towards individuals who are likely to lead a life of crime and may even re-offend. So the only ground that was held void in this case was that of "domiciliary visits at night" because then the right to property existed and they wanted to secure a person's property from trespass. Although narrowly enough, the court somewhat recognized the right, basing it on liberty founded under Article 21 but did not frame so as a fundamental right.

Justice Subba Rao, in his dissenting opinion in *Kharak Singh.*[20] drew the same inference and said that an individual even if he's a "history sheeter" in the eyes of the police doesn't deserve to live under the constant threat of being bombarded by the police by way of domiciliary visits or constant tracking his movements. He made this situation to an analogy with "the whole country is a jail". This powerful dissent laid the seed of an important observation that surveillance is called so because it's in secret and something can't really hurt you if you are not aware of its existence. But the constant looming cloud of being watched is like living in shackles. This dissenting opinion was in major disagreement with the majority that was of the opinion that Part III should be read altogether and not understood in a "silos approach" which is a contribution of the landmark judgment of *A.*

[20] Ibid. n.17

K. Gopalan[21]. Although the majority thoroughly disagreed with Justice Subba Rao's dissent, he made valid points that state surveillance is targeted and inflicts a psychological turmoil on an individual. The "silos approach" also did not see fruition for long and was rejected by the Supreme Court in *R.C. Cooper*[22] and *Maneka Gandhi*[23] and it was an accepted proposition that Part III of the Constitution has to be interpreted with the widest interpretation possible and to not in any case alienate them from each other. They derive strength and meaning from one another and validate each other's causes. It is safe to conclude here that overruling the *Kharak Singh* judgment by *Puttaswamy* was reviving the dissenting opinion of Justice Subba Rao, who understood the implications of state surveillance on privacy fifty five years ago.

After *Kharak Singh*, the next case was *R.M. Malkani v. State of Maharashtra*[24], in which the court held that recording a person's telephonic conversations is not violative of Article 21. The court held that Article 21's clause of "procedure established by law" cannot be invoked here because a telephonic conversation is not pre-meditated or staged. Whatever a person converses on the phone is under confidence that he's not incriminating himself so the conversations of innocent citizens shall be protected by the court and not otherwise for guilty citizens. The important observation here is that of the targeted "guilty person". The saving grace of this case was that it mentioned "guilty person" and this became the decisive factor in this case, the distinction of innocent and guilty.

[21] A. K. Gopalan v. State of Madras, , 1950 AIR 27
[22] R.C. Cooper v. Union of India, 1970 AIR 564
[23] Maneka Gandhi v. Union of India, 1978 AIR 597
[24] R.M. Malkani v. State of Maharashtra, (1973) 1 SCC 471, 476

Subsequently, a year later came the case of *Pooran Mal v. Director of Inspection (Investigation)*[25], the Court reinstated its position from *M.P. Sharma* and refused to add provisions akin to the Fourth Amendment.

The pivotal moment of the Indian privacy law came from the case of *Govind v. State of M.P*[26]. Just like *Kharak Singh*, it also dealt with the issue of domiciliary visits. The one point of difference in *Govind* was that the regulation was a statutory law and not an executive action. Section 46(2) (c) of the Police Act allowed the State government for such police surveillance. Since this section was "law" to that extent it could be found violative of Article 19 and 21. But even then the court did not expressly state the existence of the right to privacy. The Court relied on two tests to give a judgment. One was based on the US Supreme Court's verdict in the case of *Griswold v. Connecticut*[27] and *Roe v. Wade*[28]. From these cases the court borrowed the "compelling state interest" test which states that public interest is subject to restrictions of the provisions of Part III and hence the use of the word compelling here means to add emphasis on- "*even if it be assumed that Article 19(5)* [restrictions upon the freedom of movement] *does not apply in terms, as the right to privacy of movement cannot be absolute, a law imposing reasonable restriction upon it for* compelling interest of State *must be upheld as valid.*"

The other test that the court borrowed was from the case of *Grutter v. Bollinger*[29] of the US Supreme Court is the *"narrow tailoring"* test. This test states that the it is State's

[25] Pooran Mal v. Director of Inspection (Investigation), (1974) 1 SCC 345.
[26] Govind v. State of M.P. (1975) SCC (Cri) 468
[27] Griswold v. Connecticut and Roe v. Wade ,14 L Ed 2d 510 : 381 US 479 (1965).
[28] Roe v. Wade 35 L Ed 2d 147 : 410 US 113 (1973).
[29] Grutter v. Bollinger, 539 US 306, 333 (2003).

prerogative to demonstrate that while exercising their powers, they are infringing the rights as narrowly as possible in order to achieve their objectives.

The Supreme Court showed immense wisdom in this case and adopted the middle ground. Thus the Court upheld the constitutionality of the State's objectives by "narrow tailoring" the "compelling state interest". The Supreme Court at the time of giving the *Govind* judgment was unaware that it has impliedly founded privacy in the constitutional framework of our country.

After this landmark decision came the case of *Malak Singh v. State of P&H*[30]. In this case there were the following observations. Firstly, the court upheld the decision in *Govind* by affirming the right to privacy founded in the dignity of the individual under Article 21. Secondly, it affirmed that state surveillance was targeted to individuals who are susceptible to committing crimes and confirmed their position from the cases of *Kharak Singh, R.M. Malkani* and *Govind.*

After this case, the next discussion was called in the year 1993 in the case of *LIC v. Manubhai D Shah*[31], which was challenging Article 19(1) (a)'s freedom of speech and expression on the grounds that this freedom included the privacy of communications.

Next in line was the case of *R. Rajagopal*[32], which was case in which with the publishing of the autobiography of a convicted criminal aka Auto Shankar who had withdrawn his consent for publishing the book was discussed. The Court observed in this case that the

[30] Malak Singh v. State of P&H (1981) 1 SCC 420.
[31] LIC v. Manubhai D Shah (1992) 3 SCC 637.
[32] R. Rajagopal v. State of T.N (1994) 6 SCC 632, 639.

right to privacy in between private parties was not addressed in this case per se and which still needs to be addressed by subsequent judgments.

Now a list of cases that need a mention here are also involving the right to privacy but aren't popularly labeled so. The case of '*X' v. Hospital 'Z*[33]'. In this case the issue was that the hospital in question disclosed the HIV+ status of the appellant to his family which led to his social exclusion and that resulted in violation of his right to privacy. The Court attempted vehemently to lay ground for the private right to privacy but failed to only give an affirmation on the constitutional right to privacy.

Next in line of revelations in surveillance is the case of *People's Union for Civil Liberties v. U.O.I*[34] which is also popularly known as the "telephone tapping" case. This case is just as important as *Govind.* In this case the following of the Telegraph Act was challenged. The section read-

"On the occurrence of any public emergency, or in the interest of public safety, the Central Government or a State Government or any Officer specially authorized in this behalf by the Central Govt. or a State Government may, if satisfied that it is necessary or expedient so to do in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of and offence, for reasons to be recorded in writing, by order, direct that any message clear of messages to or from any person or classes of persons, relating to any particular subject, brought for transmission by or transmitted or received by any telegraph,

[33] 'X' v. Hospital 'Z' 1 (1998) 8 SCC 296.
[34] PUCL v. Union of India (1997) 1 SCC 301.

shall not be transmitted, or shall be intercepted or detailed, or shall be disclosed to the Government making the order or an officer thereof mentioned in the order."[35]

Following points are to be taken from this case. Firstly, Section 5(2) is an archaic legislation of 1885 which couldn't have anticipated bulk surveillance. Secondly, there needed to be rigorous standards to safeguard privacy when the court interpreted "public safety" and "public emergency". And thirdly, it affirms the cornerstone of all thought: that for liberty to flourish there is an aspect of all our lives that must remain private from the government.[36]

After this case there were many more that more or less followed the same path as the previous cases aforementioned. Some of them are as follows- *Collector* v. *Canara Bank*[37], in 2005, it was held that the right to privacy dealt with the privacy of persons and not places. The Court also made a reference to the US Supreme Court's case of *United States* v. *Miller* in which it was discussed that once a person gave away his rights to third party in appropriating his documents, there then, privacy doesn't arise. Next, in the case of *Directorate of Revenue v. Mohd Nisar Holia*, Section 42 and 43 of the NDPS Act was in question and citing previous cases of *Govind* and *Canara Bank*, the Court held that the right to privacy could not exist in cases of search and seizures under this Act. Then in 2008, came the judgment of *State of Maharashtra v Bharat Shanti Lal Shah*[38], in this case few provisions of the MCOCA was in question and had facts similar to that of *PUCL v. UOI.* The court gave a rather disappointed judgment as it didn't even consider "compelling state interest" and tried to re-interpret it and subsequently held MCOCA valid.

[35] Section 5(2), Indian Telegraph Act, 1885.
[36] Supra n. 27
[37] Collector v. Canara Bank, (2005) 1 SCC 496, 524.
[38] State of Maharashtra v Bharat Shanti Lal Shah (2008) 13 SCC 5

And now, this discussion shall steer towards the two most important cases that shall conclude this trajectory before *Puttaswamy.* Firstly is *Selvi v. State of Karanataka*[39] wherein the interrogation techniques involving narco-analysis and brain mapping were questioned and the court held that as far as these techniques infringed the mental faculties and processes of an individual, it violated his privacy and also rejected the state's argument that this technique served their "compelling state interest" for prevention of crime. The judgment's excerpt says- "There is absolutely no ambiguity on the status of principles such as the 'right against self-incrimination' and the various dimensions of 'personal liberty'. We have already pointed out that the rights guaranteed in Articles 20 and 21 of the Constitution of India have been given a non-derogable status and they are available to citizens as well as foreigners. It is not within the competence of the judiciary to create exceptions and limitations on the availability of these rights."

Something to note, the previous list of cases lay down that the right to privacy is in fact derogable when there is compelling state interest and yet this excerpt doesn't sit well with the previous holdings of the court.

Concluding this list is the very recent case of *Rohit Shekhar v. Narayan Dutt Tiwari*[40]. In this case, the appellant was court mandated to submit to compulsory DNA testing to determine paternity. The Court held that if the facts of the case make it impertinent to compel DNA test and if there is compelling state interest, reasonable apprehension then it shall not restrict itself on privacy grounds. The judgment's excerpt says- "forced interventions with an individual's privacy under human rights law in certain contingencies has been found justifiable when the same is founded on a legal provision; serves a

[39] Smt. Selvi v. State of Karnataka (2010) 7 SCC 263
[40] Rohit Shekar v. Narayan Dutt Tiwari, 2011 SCC OnLine Del 4076 (Delhi High Court)

legitimate aim; is proportional; fulfils a pressing social need ; and, most importantly, on the basis that there is no alternative, less intrusive, means available to get a comparable result." [41]

This excerpt leaves us inconclusive on the court's standing of striking a balance between the "pressing social need" and "legitimate aim" because these terms are inherently contradictory to each other. And hence for more clarity as to this right, is the transformational *Puttaswamy.*

3.2 Puttaswamy And Its Implications

The nine-judge bench comprising of Justices Dr. D.Y. Chandrachud, Jagdish Singh Khehar, J. Chelameswar, S.A. Bobde, R.K. Agrawal, Rohinton Fali Nariman, Abhay Manohar Sapre, Sanjay Kishan Kaul, S. Abdul Nazeer gave one of the most important and possibly the most challenging judgment[42] in the Supreme Court's history in civil rights jurisprudence. The reason it's challenging is because not only will it have an everlasting impact on the succeeding judgments to follow but also because it has laid down the foundations of a transformative landscape of constitutional interpretation. This judgment's analysis is crucial and quintessential to analyze because it discusses in great intricate detail the interplay between privacy and transparency, free speech, right to information, self-determination to name a few. Before delving into the critique and appraisal of this judgment, it is imperative to mention here that only the operative order of the judgment, plurality opinion of Chandrachud J, and the dissenting opinion of Chelameswar J have been afforded great importance.

[41] Ibid [79]
[42] Supra n. 1

This judgment spans over 547 pages and has went over to give references to some major landmark cases such as *Maneka Gandhi, R.C. Cooper, A K Gopalan, Selvi, Kharak Singh* etc.

To start off, the judgment in *M.P. Sharma v. Satish Chandra* stands overruled. M.P. Sharma only held that the IV Constitutional Amendment of the American Constitution could not be incorporated as a guarantee in our constitution. Bobde J, in his opinion states that M.P. Sharma is not acceptable because it negates the possibility that the right to privacy cannot exist on its own independent footing in our constitution. Which is later then proved otherwise by this judgment. He also says that drawing an analogy between the IV Amendment of the American Constitution and the Article 20(3) of the Constitution is baseless because the former is limited to the protection against state surveillance.

Next, the decision in *Kharak Singh v. State of U.P*. stands overruled in so far as it holds that the right to privacy is not protected by the Constitution. As it is already established by the operative order of this judgment that right to privacy is a fundamental right protected under Part III of the Constitution, the reason why this case was struck down was because there was no other ground but of privacy that could strike down the validity of domiciliary visits. Nariman J, opines that

" As the majority judgment contradicts itself on this vital aspect, it would be correct to say that it cannot be given much value as a binding precedent."[43]

Justice Bobde, Chelameswar and Chandrachud agreed that there was a "logical inconsistency" in the Kharak Singh judgment because there couldn't be any other reason

[43] Ibid [42]

to restrict police surveillance other than that of invoking the right to privacy and then the judgment goes on to declare that there isn't any right to privacy guaranteed in the constitution owing to the narrow reading of the term "personal liberty" which is a parcel of the A. K. Gopalan judgment. It is here that we find the first mention of the "silos approach" as Justice Chandrachud calls it in reading Part III holding that "each separate clause dealt with a separate right, and each clause was hermetically sealed from all other clauses" Meaning that the residual of personal liberty under Article 21 is devoid of the freedoms guaranteed in Article 19(1). The "silos approach" has been vehemently rejected by the Apex Court in R. C. Cooper and subsequently in Maneka Gandhi also.

Henceforth Justice Chandrachud summarily opines that- "the history that M.P. Sharma and Kharak Singh have set over 6 decades ago has now become a settled position about that the fundamental rights ensue from the basic notions of liberty, distinct from the rights that are protected under Article 19. It gives Article 21 an expansive hue. Moreover, the constitutionality of a law that verges on infringing fundamental rights is tested on whether it's objective affects the guarantees of freedom not on the objective of the State in framing that legislation. And lastly, Article 14 needs to be always interloped while reading of guaranteed freedoms in Part III".[44]

The next proposition of importance is the crux of the operative order which is the guarantee of the right to privacy as an intrinsic part of Article 21 and as part of the guarantees by virtue of Part III of the Constitution.

[44] Ibid. [24]

It has been repeated, rehearsed and referenced an umpteenth amount of times throughout this judgment that privacy is latent within liberty, dignity, and autonomy. Starting with the opinion of Justice Chelameswar, he grounds his opinion of liberty on three aspects which are "repose", "sanctuary" and "intimate decision" which are at the centre of the basic foundation of liberty and Article 21 and 19.[45]

Justice Chelameswar emphasizes on the broader rights of the freedom and autonomy of body and the freedom of mind.[46] This is a marvelous observation by the hon'ble justice for the advent of criminal jurisprudence. He affirms in this judgment that autonomy and freedom of the mind as well as the body is intrinsic and inalienable to the right to privacy, because what would be privacy if not of the body and mind of a person.

Justice Bobde founded his opinion on "two values, the innate dignity and autonomy of man"[47], This he said founds its place right in the constitution. He also held that privacy was a "necessary and unavoidable logical entailment of rights guaranteed in the text of the constitution"[48]. In Justice Bobde's opinion we find that the mention of seclusion that should be exercised as a matter of right under Article 21. He calls privacy "an enabler of guaranteed freedoms" [49] and "an inarticulate major premise in Part III of the Constitution."[50].

Justice Nariman opines articulately and links three aspects of privacy which are bodily integrity, informational privacy and privacy of choice.[51] This, right here, is where the

[45] Ibid. [36]
[46] Ibid [38-40]
[47] Ibid. [12]
[48] Ibid [35]
[49] Ibid [29]
[50] Ibid [25]
[51] Ibid [81-82]

"right to privacy in criminal justice administration hereinafter mentioned as CJA" gains momentum from.

He opines it in the following manner: "The dignity of an individual lies in his right to develop to the maximum of his potential; and this can only be possible if a person has full control over his choices and decisions."[52] He summarily opined that individual self development was at the heart of dignity and personal liberty and also in turn at the heart of Article 21. One of the most important observations that are made here are also that the right to privacy is meaningless without security of the body, mind and intimate choices.

Needless to say that our CJA is inclined heavily to protect the interests of the accused, it is also heavily biased in the favor of the state because the State is all-powerful. The interests of the accused are overshadowed when the State plays almighty with the fundamental rights (Part III) under the façade of overarching "public interest".

On the same lines Justice Sapre bases his opinion on "individual self-determination" who notes that dignity imposes "an obligation on the part of the Union to respect the personality of every citizen and create the conditions in which every citizen would be left free to find himself/herself and attain self-fulfillment."[53]. And Justice Kaul calls privacy "nothing but a form of dignity, which itself is a subset of liberty and key to freedom of thought"[54]

All of these opinions are brought together by Justice Chandrachud by grounding privacy in dignity and calling it the core of liberty and freedom, autonomy, bodily and metal integrity and across the spectrum of protected freedoms spanning across PART III.[55] The

[52] Ibid [85]
[53] Ibid [8]
[54] Ibid [40] [52]
[5555] Ibid [32], [34], [107], [113]

point of significance here is that the Apex Court could have chosen to interpret privacy on the basis of already existing jurisprudence but it went on to the deepest roots of constitutional spirit to expand its meaning. The court started off with the basic idea of bodily and mental integrity, then informational self determination and then to the heart of it all, the right to intimate choices founded in liberty and dignity. Privacy, therefore, was both an overarching, foundational value of the Constitution and incorporated into the text of Part III's specific, enforceable rights.

As this chapter proceeds in consequent appraisal and critique it will become more apparent that the *Puttaswamy* judgment stops at the mere declaration that right to privacy exists and does not go beyond in laying down the blueprint for upcoming challenges that the succeeding benches will face in determining the extent of the right and limiting the interferences of the State. While the privacy judgment is a cause for celebration, its full benefit will only come when it is applied to actual state actions that undermine privacy.

The next point that needs attention in this judgment is how the wordings of the judges revolve around a few terms and their meanings an in very intricate detail. The term privacy entails private spaces, which is called "private realm" in this judgment which encompasses the body and the mind and everything that surrounds it such as the right to move the body freely, the right over ones thoughts and the control over the dissemination of information. Justice Chandrachud terms this "private realm" as an area that has "spatial control", where the mind and body is free to create choices.[56] This view is shared by his brother judges also wherein they agreeable conclude with him that for privacy of the mind and body and

[56] Ibid [85] [53]

the space surrounding it, the individual is at the heart of it all. Justice Chandrachud summarizes it as privacy has many facets and intricacies such as spatial control, decisional autonomy and informational control.[57] Decisional autonomy is the freedom of choices whereas informational control is the privacy to shield personal information from public disclosure. It is here that the justices make a reference to the first initial case that began this debate of the right to privacy which is *Govind v. State of MP*. In this case it was held that "any right to privacy shall protect the institutions such as marriage, home, family, motherhood, procreation and child bearing." On paying attention to each of these words, we realize that they denote a private places or institutions and the individual here is just a part of than institution, so by extension we can say that this privacy here is of the spaces and not the individuals and the privacy has been about physical or functional setups. This is not a criticism because privacy in private spaces is just as important because we would frown upon the state's interference in matters of family and marriage. What needs pondering over is that if "walling off" private institutions begins at the physical and institutional doorstep of a person's home, then what might have been going on inside those doors that maybe requires a little attention from law enforcement. On this same point, it is pertinent to mention the case of *T. Sareetha v. Venkatasubbaiah*[58] wherein the section 9 of the Hindu Marriage Act 1956 was challenged and struck down by the Andhra Pradesh High Court on the ground that this section was unconstitutional on the ground that State interfered with a woman's decision to engage in sexual intercourse with her spouse, and seems like a legitimate explanation too but, this section was subsequently upheld by the Delhi High Court on the grounds that the restitution of conjugal rights between a husband

[57] Ibid [142]
[58] T. Sareetha v. Venkatasubbaiah AIR 1983 AP 356

and wife was their private matter and didn't instituting constitutional grounds inside a family home. It also held that Article 21 and 14 do not find place in the four walls of a marriage because it can weaken a wedding vow. If this isn't an outrageous finding then wait till it got more validity from the Apex Court wherein they upheld the decision of the Delhi High Court and held that the provisions of the constitution mustn't destroy a marriage or aid in it.

What inference can be drawn from this case is that the Andhra High Court understood privacy but also understood where it didn't have to be a shield to protect patriarchal orthodoxies. The Andhra High Court understood that liberty and privacy was in the freedom of choice. What Delhi High Court misconstrued (for the lack of a better word) is privacy in "spatial control" and what goes on in a family home and between marriages is also privacy. Which isn't completely flawed because it is, the point is balance, striking balance between the privacy of spaces and the acts committed in the safety of those spaces.

Justice Chandrachud goes on to say that the idea of the framing of this right to privacy is not just morally correct but also constitutionally sound, because it can't be studied in isolation from the golden triangle. That brings us to what the initial observation was and the most important one, which is, the individual remains, the most basic entity, and he shall alone be the bearer of this right to privacy.

Next important aspects of this judgment are three terms that need attention. These are personal information, decisional autonomy and informational self-determination. Starting off with what constitutes the individual and how shall his privacy be safeguarded. To answer this question, an individual has mass and occupies space so he's matter, which means his physical body and the other thing is the engine that keeps him going which is

his mind. The body is invariably the most crucial to the right of privacy. Justice Chelameswar[59] talks about the privacy in context of bodily integrity and calls it "freedom from unwarranted stimuli". This phrase finds its place in the much discussed judgment of *Selvi v. State of Karnataka*, where creative police interrogation techniques such as brain mapping and narco-analysis as a violation of the mental privacy under Article 20(3) and Article 21. The privacy isn't just interference by the state directly invading homes, but beyond that. In 2013, after Edward Snowden disclosed groundbreaking information about the State surveillance programs of the United States that led to a chain reaction which led to a large amount of privacy and bulk surveillance discussions in India. Glenn Greenwald in his book on Snowden's adventures made the following remark about the State surveillance in the United States- *"Only when we believe that nobody else is watching us do we feel free – safe – to truly experiment, to test boundaries, to explore new ways of thinking and being, to explore what it means to be ourselves… for that reason, it is in the realm of privacy where creativity, dissent, and challenges to orthodoxy germinate. A society in which everyone knows they can be watched by the state – where the private realm is effectively eliminated – is one in which those attributes are lost, at both the societal and the individual level."*

This view is congruent to an observation made by Bentham in his *Theory of Panopticon* wherein he states that a person (in his example, a prisoner) will never be certain if he's being watched or not. Meaning that power and the exercise of that power should be visible and not in secret leaving the person in a constant state of angst. On this note, Justice

[59] Supra n. 1 [36]

Chandrachud notes[60], *"*Individual dignity and privacy are inextricably linked in a pattern woven out of a thread of diversity into the fabric of a plural culture."

What can be concluded from these set of opinions is that which Justice Subba Rao hold in his dissenting opinion in *Kharak Singh* in which he says that all the guaranteed freedoms which we get from our constitution stand diluted without privacy. Privacy is multi-faceted and to understand it, it should be read with pluralism, democracy and diversity of an individual as a separate entity and an individual as a member of a society.

In this judgment, informational self-determination is discussed by Justice Kaul and Justice Nariman and in the plurality opinion of Justice Chandrachud. They hold that Informational self-determination is strictly restricted to a person's mind and the information that he stores in it voluntarily or otherwise. Informational self-determination means that when a person has been afforded the right to privacy that shall also afford him control over all the information that's personal to him and also the dissemination of that information. This issue is inextricably intertwined with the data protection also. The judgment on the point of informational self-determination is very clear- it solely relies on informed consent as the basis. Justice Chandrachud highlights it by noting that autonomy is one of the pillars on which privacy stands and that needs to be protected. So if informed consent and right to privacy are two peas in a pod then we can conclude that, consent is not a waving your right of control over your information and extends to each and every use of that personal information. Therefore, voluntarily giving away your information to the State does not mean that it's state's sanction to do what it may with that information. Because the

[60] Ibid. [168]

constitutional provisions binds the State to be responsible towards the individual and inform him of the various stages of use of his information.

One of the commendable qualities of the Supreme Court of India is that it doesn't consider its' decision to be set in stone and is constantly evolving by changing its previous judgments. This is pertinent to mention to understand the next important concept in this analysis which is decisional autonomy. Justice Bobde[61] and Justice Nariman[62] call this decisional autonomy as the centrality of "Choice". They state that- "privacy of choice… protects an individual's autonomy over fundamental personal choices"[63]. This they interlinked with the concept of democracy because to be truly democratic one must exercise his choice from free will. For a personality to grow, for a person to truly develop, he needs to have the control over his intimate choices and decisions and these can only take place in personal spaces.[64]

A major part of this judgment went into elaborating greatly on the term choice and how it affects a person. Examples of the case of *Koushal v. Naz Foundation*[65] were referenced, the *Akhila/Hadiya case* was also referenced to emphasize on the issue of freedom of choice.

Now the point of focus shall be the Limitations of the *Puttaswamy* judgment. We have successfully established that the right to privacy is not an absolute right, so now we need to map in what events the State will be prevented on the grounds of the violation of privacy. The Supreme Court did marvelously on two fronts. Firstly, it held the forty years of

[61] Ibid. [31]
[62] Ibid.[81]
[63] Ibid. [81]
[64] Ibid. [85]
[65] Suresh Kumar Koushal v. NAZ Foundation and Ors., AIR 2014SC 563,

previous jurisprudence valid and secondly, by laying down specific new standards. For this we refer to the operative order[66] of the order which states that *"*the right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution." [67] continues: "Decisions subsequent to *Kharak Singh* which have enunciated the position in (iii) above lay down the correct position in law."

Here there are two observations, first is the recognition of privacy within the ambit of Article 21 and the other is guaranteeing it as part of fundamental rights (Part III) of the Constitution. This is tricky because Article 21 also forms part of Part III. The court singled out Article 21 because the basis of this right stems from the right to life and personal liberty and the other articles that have facets of privacy such as Article 14, 19 and 25 provide for lenient limitations as compared to that of Article 21. Justice Nariman opined[68], *"*... when it comes to restrictions on this right, the drill of various Articles to which the right relates must be scrupulously followed". Justice Kaul held that[69] "let the right of privacy, an inherent right, be unequivocally a fundamental right embedded in part-III of the Constitution of India, but subject to the restrictions specified, relatable to that part." And Justice Bobde opined[70] "once it is established that privacy imbues every constitutional freedom with its efficacy and that it can be located in each of them, it must follow that interference with it by the state must be tested against whichever one or more Part III guarantees whose enjoyment is curtailed".

[66] Supra n. 1 [3]
[67] Ibid. [4]
[68] Ibid. [86]
[69] Ibid. [83]
[70] Ibid.

One of the most important limitations was given by Justice Chelameswar. He held that "the limitations are to be identified on case to case basis depending upon the nature of the privacy interest claimed."[71]

So to draw inference, The majority in *Puttaswamy* held that the violations to privacy under Article 21 must satisfy the grounds of just, fair and reasonable as established in *Maneka Gandhi.*

3.3 Aftermath of The Puttaswamy Judgment- What Lies Ahead

From the earlier discussions it is safe to conclude that *Puttaswamy's* judgment can actually make concrete difference if it is thoroughly applied by succeeding benches. It is one of the most elaborative and judicially sound judgments of the Supreme Court that has discussed the constitutionalism of over four decades. The way to heaven is paved with stones can be said for the benches that will have to follow in the footsteps of this judgment and it will not be an easy task because this judgment still hasn't answered many questions and still leaves a lot of stones unturned. There is much reference in the judgment of the constant evolving nature of the Constitution and how it's a "living and breathing document". Justice Kaul authors a chapter titled "*The Constitution of India – A Living Document*"[72] within this judgment. Yes it has been argued in this case that the constitution grows but to what and where to? The judges are bestowed with this prestigious responsibility of adapting and changing with the time, the spirit of the constitution.

[71] Ibid. [46]
[72] Ibid. [23-49]

It would be remiss to mention that this judgment overruled the landmark judgment of *ADM Jabalpur v. Shivakan Shukla aka Habeas Corpus* case. The Court previously has upheld the suspension of the writ of habeas corpus during emergencies. The majority as well as the plurality in *Puttaswamy* overruled this judgment on the ground that some rights pre-exist the constitution and those are "natural rights" inherent in every person. To this Justice Chandrachud draws the analogy that *"*privacy is a concomitant of the right of the individual to exercise control over his or her personality. It finds an origin in the notion that there are certain rights which are natural to or inherent in a human being. Natural rights are inalienable because they are inseparable from the human personality. The human element in life is impossible to conceive without the existence of natural rights*."*[73].

One of the biggest critiques of this judgment is that it only talks about the right to privacy against the intrusive action of the state and there is no mention of what the status of this right will be against other rights such as the freedom of speech and expression and by extension is the right to seek information. Section 8 (j) of the RTI Act gives exemption from disclosure. It says- "… information which relates to personal information the disclosure of which has no relationship to any public activity or interest, or which would cause unwarranted invasion of the privacy of the individual unless the Central Public Information Officer or the State Public Information Officer or the appellate authority, as the case may be, is satisfied that the larger public interest justifies the disclosure of such information."

[73] Ibid. [40]

The judgment is completely silent on what implication it has on provisions such as this which only provide for exemption unless there is a compelling state or public interest. The judgment is also fairly silent on describing the term "personal information" which proves problematic for a lot of legislations that shall rely on it for securing privacy safeguards.

CHAPTER 4

INTERNATIONAL PERSPECTIVE ON DNA PRIVACY

4.1 DNA DATABASES- UNITED STATES OF AMERICA

Three decades after the discovery of the double helix structure of the deoxyribonucleic acid[74] (hereinafter referred to as DNA) , it became a gold standard for forensic evidence in the United States. It is such a crucial piece of evidence in homicide and sexual assault cases that it is in many instances relied solely upon to base a conviction. Since the advent of DNA technology, there has been a need felt to grow the portal that stores this DNA evidence. This need has even let some to go far as proposing to have DNA collected from every single American hence forming a universal DNA database.

The credibility of DNA as evidence is nearly perfect which has led to the recognition of its utility in the criminal justice systems. The proponents of the Universal DNA database say that DNA evidence is flawless in truth-finding and reliability because it has proven to be Holy Grail evidence in numerous convictions in the United States[75]. Because of the advancements in this technology there is more and more support in favor of using this evidence in criminal trials. Many scholars and scientists such as Eric Posner, Arnold Loewy and Andrea Roth[76] have advocated in favor of these databases stating that they will prove incredibly valuable. They are of the opinion that this shall strengthen law enforcement and will provide for better security. They also stress on the point that every American citizen must dutifully provide his DNA for these databases to make the criminal justice administration more effective.

[74] Meghan J Ryan, "The Privacy, Probability, and Political Pitfalls of Universal DNA Collection" (2017) 20:1 SMU Science & Technology L Rev 3
[75] Ibid. *see* also Maryland v. King, 133 S. Ct. 1958, 1966 (2013) (stating that "[t]he advent of DNA technology is one of the most significant scientific advancements of our era" and that "the utility of DNA identification in the criminal justice system is already undisputed").
[76] Infra n.70

These supporters have also recognized that this universal collection of DNA imposes widespread privacy safeguards to be addressed. But they ultimately are of the view that the benefits of universal databases outweigh the cons because they contend that this is constitutionally sound under the IV Amendment of the US Constitution.[77][78]

To comprehend the intricacies of DNA databases it is important to understand their progression through time in various states. All the 50 states in the USA have some or the other form of DNA database and every state permits the DNA data banking of some samples also. The latest data reveal that as of July 2005, 43 states take the DNA samples under the "all the felonies" category, 28 states take DNA samples from juveniles and 38 states have various filters titled "misdemeanors". [79]

An important questioned needs answering. Whether DNA samples should be retained by the State?[80] Currently in the US, there are federal as well as state policies respectively that govern DNA collection. The Privacy Act Notice on the NDIS[81] states that it shall safeguard the DNA samples and at the federal level is the FBI's CODIS (Combined DNA Index System)[82] and their quality assurance is that they "shall retain the DNA sample indefinitely for the purposes of finding a potential match from a sample collected at a crime scene". Similarly, almost all 50 states retain the DNA samples in their respective databases

[77] Arnold H. Loewy, A Proposal for the Universal Collection of DNA, 48 TEX. TECH L. REv. 261, 267 (2015)
[78] Andrea Roth, Maryland v. King and the Wonderful, Horrible DNA Revolution in Law Enforcement, 11 OHIO ST. J. CRIM. L. 295, 308-09 (2013)
[79] R.E. Gaensslen, Should Biological Evidence or DNA be Retained by Forensic Science Laboratories After Profiling? No, Except Under Narrow Legislatively-Stipulated Conditions, 34 J. L. MED. & ETHICS 375,377 (2006).
[80] Natalie A Bennett, "A Privacy Review of DNA Databases" (2008) 4:3 I/S: A J of L & Policy for the Information Society 821.
[81] Privacy Act of 1974, U.S.C. §552a (1996); New System of Records, 61 Fed. Reg. 139, 37495 (1996).
[82] David H. Kay, Please, Let's Bury the Junk: The CODIS Loci and the Revelation of Private Information, 102 Nw.U. L. REV. 70, 71 (2007)

indefinitely, for example the State of Nebraska holds DNA samples for time immemorial, whereas some states have the policy to expunge this sample if a convict is exonerated or his case is dismissed[83]. For instance, the State of Wisconsin is the only state that mandates that the DNA samples be destroyed after they have fulfilled their purpose[84]. The State of Arizona holds it for thirty five years before destroying, in the hopes that they can solve unsolved sexual assaults and homicides[85]. There is no federal policy in place that requires the state or the CODIS to destroy DNA samples after a certain time period and that raises serious privacy concerns because of the amount of information that the DNA provides. Also, because there a lot of private laboratories or third-party business involved in the DNA identification and analyzing process that it could easily be misused. [86]

Now, the focus should be on what kind of DNA can be stored. To understand this, we shall consider DNA sample analogous to a fingerprint sample. But like a fingerprint *only* identifies a person, DNA can provide a huge spectrum of personal information such as his family history, hereditary, ancestry, his characteristics and features, any pre-disposition to diseases etc. The DNA that is usually used as evidence is termed as "junk DNA"[87] because it is non-coded and law enforcement is not equipped to understand whether it performs and important functions or not. But as mentioned earlier there is no personal information other than an index number specifying the DNA sample is stored on the NDIS. The Federal DNA Identification Act limits the disclosure of the DNA samples stored in the NDIS and

[83] Nebraska Revised Statutes Chapter § 29-4105 (2005). Nebraska Legislature
[84] Wisconsin Statutes Table of Contents. § 165.77 (West 2004 & Supp. 2007)
[85] Arizona Revised Statutes Chapter§ 13-610 (LexisNexis 2005). Arizona Legislature
[86] Barry Steinhardt, Privacy and Forensic DNA Data Banks, in DNA and the Criminal Justice System: The Technology of Justice 190 (David Lazer ed., The MIT Press 2004);
[87] Colloquy, Is the "JUNK"DNA Designation Bunk?, 102 NW. U. L. REv. 54,56 (2007).

CODIS.[88] Majority of the states in the US have some kind of provision to ensure the confidentiality of the DNA samples such as if there is any illegal or unauthorized acquisition of DNA, then there is a penalty of $250,000 and imprisonment for a period not extending one year. 38 states have imposed such penalties and 18 states penalize such offenses under a felony charge. Therefore, irrespective of what kind of DNA sample is retained or in which database, as long as there are samples from such a large population retained under databases with no uniform federal policy, there will always be looming privacy infringement concerns. It is up to the state to balance the rationale behind retaining DNA samples for larger public interest and individual privacy.

The next important point of concern is who should be giving samples? Some supporters of the universal database advocate that irrespective of a person's actions, age, and occupation or otherwise, their DNA should be stored by the government. They say that this shall deter crimes because there will be a constant threat of the state and people will be *less likely* to be committing an offence knowing that they could be very easily apprehended, which is sound reasoning, but only as far it wants to create a deterrence, but the whole idea behind having to store DNA was based on the fact that suspects, offenders, convicts and arrestees would be ones whose DNA would be stored to rule them out as part of elimination or to convict them by comparing DNA found at crime scenes. To have the entire population submit themselves to DNA testing seems far-fetched. Some privacy advocates are of the opinion that the so called misnomer of "junk DNA" which reveals a great deal of personal information about a person, will also let the law enforcement agencies know whether a

[88] M. Dawn Herkenham, Retention of Offender DNA Samples Necessary to Ensure and Monitor Quality of Forensic DNA Efforts: Appropriate Safeguards Exist to Protect the DNA Samples from Misuse, 34 J.L. & 380, 381 (2006). Med. Ethics

person has the genetic disposition of committing a crime, or whether he is susceptible to HIV that could possibly endanger the well beings of others, and based on the state's "overbearing public interest" they will get access and permission to indict a person based on his genetic composition.

The whole bandwagon of universal DNA database began when the New York mayor Rudolph Guilani, in 1999 proposed that DNA samples should be collected from newborns for law enforcement purposes. His idea was also based on the thinking that this will strengthen the law enforcement agencies and somehow this "not-so-exact" science of predictions will help prevent a crime before it happens.

Realistically, it is not impossible that such a database will exist. But what can't be ignored is that we will never be one hundred percent sure of what the government wishes to do with such vast amount of personal information. This fear of privacy infringement goes beyond criminals and history sheeters, but is also founded in many innocent Americans. There is a possibility that this private information is sold to healthcare facilities or pharmaceutical companies so they could target potential clients or even to insurance companies that can hoax a person by disclosing them information about their probable mortality rate etc.

Because most of the policies take shape and form because of the tax payer's money, to have a nationwide DNA database will require copious amounts of money and resources, not just for DNA sample collection and storage but also to ensure the credibility of the sample, its contamination, transport and viability. And the biggest problem of all which some term as "mission creep", which is once there is a universal database, there is no telling what the politicians of the country wish to do with that information.

4.1.1 THE FOURTH AMENMENT

The infallible quality of DNA evidence is undisputed by many. What now needs to be addressed is whether the DNA samples can actually improve the investigation in criminal cases is more important or the fact that in this process we might be offending the individual's privacy. To start off, it can be rebutted that DNA evidence is not one-hundred percent reliable in crime solving. For instance, it cannot be ignored that there is huge risk of contamination of crime scenes during collection of evidence, a mix-up of samples of the police officers, innocent bystanders, victims and the perpetrators, a chance that the technician testing the samples made an error and the biggest possibility that a matching DNA profile doesn't necessarily mean guilt. So, it is safe to infer that DNA, just like any other forensic evidence can lead to misleading results.

In the landmark case that began this debate of DNA privacy, *Maryland v. King*[89], in 2013, the US Supreme Court for the first time inquired into the constitutionality of compelling arrestees to submit to DNA testing. The advocates from the side of the state argued that this was routine booking procedure under the Fourth Amendment and the court upheld this argument. The bench comprised of five judges out of which four namely Justices Scalia, Ginsburg, Sotomayor and Kagan, warned the implications of this ruling. They penned in their opinions that this judgment gives constitutional protection to the government to "take your DNA and enter into a national database, if you are arrested, rightly or wrongly and for whatever reason".[90] It is only the opinion of Justice Kennedy that supports the views

[89] Vikram Iyengar, "Maryland v. King: The Case for Uniform, Nationwide DNA Collection and DNA Database Laws in the United States" (2014) 23:1 inf & Comm Tech L 77.
[90] David H. Kaye, 'Why So Contrived? The Fourth Amendment and DNA Databases after *Maryland v King'* (2014) 104 J Crim L & Criminology (forthcoming) http://papers.ssrn.com/sol3/papers.cfm?abstract id=2376467

of the proponents of universal DNA database and says that it will "improve pre-trial court and police procedures".[91] Although the other four judges are clearly not on-board with the DNA sampling but the judgment lacks any rational reasoning behind their dissent of taking DNA *sans warrant.*

Before *King's* case, the US Supreme Court had received plenty of appeals from convicted felons and arrestees to address the constitutionality of the DNA sample collection that the state call "routine procedure". These requests led an inquiry which revealed that the poor State and federal laws that govern DNA databases. For instance, in California, the people passed the Proposition 69 which requires DNA sampling for "all felonies". This includes petty crimes also such as theft, drug possession, subleasing a car or even joyriding. [92]

This is just one of the examples of one of the populous states of the US. A citizen's legitimate expectation of privacy from the legislature, which is desirable and also reasonable, is very different from what a judge perceives in a case. The Fourth Amendment doesn't recognize informational secrecy or decisional autonomy as the prerequisite to privacy. The words of the Fourth Amendment[93] say that it protects the citizens from any search or seizures, and the involuntary DNA sampling and storing indefinitely in the National Databases is clearly an unlawful seizure. What is needed is an executive action combined with the Congressional approval to establish a nationwide policy. [94]

4.2 DNA DATABASES- UNITED KINGDOM

The United Kingdom (hereinafter referred to as the UK) has one of the oldest and most

[91] Supra n. 75
[92] (citing Plaintiffs-Appellants' Supplemental Brief Re Maryland v. King, Haskell v Harris, No 10-15152, 1 July 2013, at 3).
[93] US Const. amend. IV.
[94] Supra n. 75

extensive DNA databases in the world. Since its inception in 1995 it has the samples of over 4.5 million individuals which is over 7 percent of the entire population of UK. These samples range from those of criminals convicted of serious crimes, petty crimes, suspects, under trials and even children as young as 10 years old. There are many reasons why England and Wales has the largest DNA database in the world, out of which the most important is that Britain does not have a written constitution and hence there are no written set of fundamental rights or a bill of rights synonymous to the US that can guarantee the right to privacy like other countries. According to eminent scientists Robin Williams and Paul Johnson, the National DNA Database (NDNAD) is not authorized by any legislation and an initiation to have a legislative control in 2008 resulted in expansion of police powers to procure DNA. [95]

4.2.1 S AND MARPER V. UNITED KINGDOM [2008] ECHR 1581[96]

As the brief history aforementioned suggests, the Police in the UK had the power to retain DNA samples from accused persons even after they were acquitted or the charges against them were dropped against them subsequently. This is a landmark case that recognized the violation of privacy that can arise from this indefinite retention of DNA samples. The case involved two people who were charged with armed robbery (Mr. S) and harassment (Mr. Marper) whose samples were taken in 2001 and they were both acquitted in a few months time. Both the plaintiffs had requested that their samples be destroyed and filed an

[95] Robin Williams and Paul Johnson, "Inclusiveness, Effectiveness and Intrusiveness: Issues in Developing Uses of DNA Profi ling in Support of Criminal Investigations," Journal of Law, Medicine and Ethics 33, no. 3 (2005): 545– 558, quotation at 547, 07/07/2020, 12:07 am, http:// www.ncbi.nlm.nih.gov/pmc/articles/PMC1370918/pdf/nihms-6441.pdf

[96] Dr. Helen Wallace, statement in the Grand Chamber of the European Court of Human Rights Between "S" and Marper v. The United Kingdom, application nos. 30562/04 and 30566/04.

application for the same. The application went through avenues and the Court of Appeal held that the Chief Police Constable, if he is sure that no suspicion exists can have the DNA samples removed or destroyed. [97]The appeal finally reached the House of Lords in 2004 which is the first time the court realized the implication of retaining DNA samples of individuals who are proven innocent. The House of Lords emphasized on the CJP Act 2001 and said that the holding of DNA samples indefinitely is a violation of the right to privacy under Article 8 of the European Convention on Human Rights which is also a testament to the fact that it constitutes the interference of state with the right of an individuals' private life, but the court was also of the opinion that the pros of having a national database outweighs the cons of the violation of rights because the database acts a crime deterrent.

The case then went to the European Court of Human Rights in 2008 and the court unanimously held that the indefinite retention of DNA samples of individuals who aren't convicted of any offense stand s in violation of Article 8 and is a violation of their right to privacy.

In this case the court set the ground for the recognition of the right to privacy when it concerns DNA material. Because the definition of DNA is so wide and hugely interpretive that it is almost impossible to secure private information.

4.3 DNA DATABASES- JAPAN

[97] S. and Marper v. The United Kingdom, 30562/04 [2008] ECHR 1581¶ 69, 07/07/2020, 12:17am http:// www.bailii.org/eu/cases/ECHR/2008/1581.html

Under Article 35 of the Constitution of Japan, the word "search" constitutes taking a DNA sample. Japan has had a functional DNA Database from 2004 which is under the National Police Agency (hereinafter referred to as NPA) which came into existence with the objective that the Suspect DNA profiles shall be stored and this shall only be used as an aid in criminal investigations. The Criminal Investigation Bureau is in charge of this database and is monitored directly by the Director. The Japanese database has all varied kinds of DNA a sample ranging in age and demographics, but the important point of distinction is that these DNA samples are not used for anything else such as identification of deceased persons or paternity disputes and is exclusively saved for criminal investigations. As far as the size of this database is concerned it considerably small and is about 0.008 percent of the country's population which is lesser than 2.7% of the US Population and even lesser than 7 % of the population of UK. [98]

THE ASHIKAGAA CASE[99]

In the year 1990, near the banks of river Watarase in Ashikaga, Japan, the body of a four year old girl (Mami Matsuda) was discovered, naked, with traces of DNA on her clothes and around her mouth. The police arrested a suspect by the name of Toshikazu Sugaya on suspicion and collected his DNA sample from his garbage. His sample was a match to the one found at the crime scene, he was indicted and was sentenced to prison for murder in the year 1993. His counsel argued profusely about the viability of the DNA evidence and the fact that it was an unreliable source of evidence. Sugaya's counsel also contended that

[98] Japan Federation of Bar Associations (JFBA), "Opinion on the National Police Agency DNA Database System 07/07/2020, 12:26 am, http://www.nichibenren.or.jp/en/activities/statements/071221.html
[99] Hosokai (Lawyers' Association), Admissibility of Expert Evidence based on MCT 118 DNA Analysis-*Ashikaga* Case, Adjudicated on July 17, 2000 (2003), summarized and translated by E. Omura, January 2008.

the DNA obtained from the garbage was illegal search without a warrant. The case in 2000 was heard in the Supreme Court and it upheld that DNA as evidence is a reliable source of evidence and there was no illegal search when the sample was collected from the garbage.[100] Sugaya's counsel then went on to request the DNA to be tested again and again and even requested a retrial. Finally after much of their perseverance, the Tokyo High Court in 2009 reordered the re-examination of the DNA evidence and it was revealed that it was in fact not a match to Sugaya. Up till this point he had served a 17 year imprisonment. Finally after much wait, Sugaya was released from prison and acquitted from all charges.

This case is known as the first case that overturned a conviction after DNA testing. This case is important from the perspective of right to privacy because it highlights something very unique and unheard of in the previously mentioned cases which is the right of an individual post conviction DNA testing, where the sole basis of conviction was DNA testing.

4.4 DNA DATABASE-GERMANY

Germany was initially a reluctant participant to the whole DNA database bandwagon, and it's reluctance was well founded on the privacy concerns and the risk of violation of personal data. But there were a series of highly scandalous case of sexual assault on children in 1996-1997 that led to the German Minister of Justice to take action. Therefore in the year 1997, the Statute on Identification Through DNA Testing was passed and a

[100] Court Rejects Retrial Request from Man Convicted of Killing Girl Through DNA, "GaijinPot .com, February 13, 2007, 07/07/2020 01:22 am, http://gaijinpot.com/search/index/lang/en?q=court+rejects+retrial+request

supplementary amendment to their Criminal Procedure Code too that birthed their DNA database. [101]

CHRISTINA NYSTCH MURDER CASE

One of the most important cases in DNA testing in Germany is the case of the 11 year old Christina Nystch who disappeared on her way home and her body was discovered five days later in the forest near her home in Strucklinge. When the police ruled her death as a murder, a series of DNA sample collection began and it led to what's today known as the largest DNA dragnet in the world. At the end of this search, over 16,400 men between the ages of 18 and 30 were tested for samples. The killer (Ronny Riken) was eventually caught in 1998 when his DNA matched the one recovered from the victim's body , following which he confessed to having raped Christina and was subsequently charged with the rape of another 11 year old girl.[102]

This case led to the incarceration of one of cruelest criminals lurking in the world and it was all possible due to the DNA sampling. A large chunk of the population at the time opposed this DNA dragnet because it was inconclusive as to why so many men were being profiled whereas very limited information was available as to the offender. The DNA match to Ronny Ricken was a one in ten thousand chance that actually did get caught.

The uniqueness to the Germany's DNA databank is that it has provided for various procedural safeguards as compared to the US and UK. It calls for destruction of DNA

[101] German Code of Criminal Procedure, Section 81g [DNA Analysis] (2) 08/07/2020 11:34 am, http://www.iuscomp.org/gla/statutes/StPO.htm#81g

[102] Hermann Schmitter and Peter M. Schneider, "Legal Aspects of Forensic DNA Analysis in Germany," Forensic Science International 88 (1997): 95– 98, citing Neue Juristische Wochenschrift (NJW, translated as New Legal Weekly) 1990, 2944– 2945, http://rsw.beck.de/rsw/shop/default.asp?site=njw

samples of the individuals who has volunteered their samples, the convicted felons and the suspects all alike must be destroyed after they have served their respective purposes and their profiles have been created. In the German DNA database, the DNA profiles are also removed and destroyed after a person has been acquitted or against whom all charges are dropped automatically. [103]

CHAPTER 5

ANALYZING THE DATA PRIVACY- PERSONAL DATA PROTECTION BILL 2019

[103] Martin Kreickenbaum, "Germany: Expansion of DNA Testing— A Step Towards Genetic Registration," World Socialist Website, February 24, 2005. 08/07/2020 12:10 pm, http://www.wsws.org/articles/2005/feb2005/dna-f24.shtml

5.1 PROVSISIONS OF THE BILL- A CRITIQUE

The preamble to this act begins with the assertion that "the right to privacy is a fundamental right" and hence it is pertinent to protect personal data as an essential facet of informational privacy. The preamble also goes on to elaborate on the objective that protection of the autonomy of every individual's personal data and the appropriate use of this data if the need so arises, to ensure the accountability of said data and provide necessary remedies in case this data is misinterpreted and the most important, to set up a Data Protection Authority.

Personal data according to this act is data that is either about or in relation to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, or any combination of such features, or any combination of such features with any other information. Justice B. N. Srikrishna Committee was vested with the task to scrutinize the data protection bill. It submitted a report titled "A Free and Fair Digital Economy- Protecting Privacy, Empowering Indians"[104]

The highlights of the report and the bill are summarized as follows.

The committee emphasizes on the "purpose" of the data collection and says that it shall be lawful and necessary to qualify for collection. The transactions related to personal data must be handled with utmost care. The committee draws attention to the point where in the bill, this data can be collected from a citizen for fulfill any purpose as the Central Govt. or

[104] Anirudh Burman, Will India's Proposed Data Protection Law Protect Privacy and Promote Growth? The Growth of Privacy Regulation and the Bill , Carnegie Endowment for International Peace (2020) , 10/06/2020 01:13 pm , https://www.jstor.org/stable/resrep24293.4

the State Legislature may deem fit and remains silent on the ambit of said purpose which goes without saying that this could lead to misuse and violation of the consent of the citizen as anything and everything can be cloaked as "necessary" by the State and Central legislature on their whims and fancies.

One of the more positives among the recommendations of the committee is the "right to be forgotten" to the person consenting to give his personal data also referred to as "data principal". This means that the "data principal" has the right to restrict or prevent any display of its personal data after the need for such data has expired.[105] This "right to be forgotten" is derived from the EU where it has been used by "data principals" to withdraw their consent from disclosure of their personal information once its necessity has been fulfilled. This right is one of many afforded to the citizens consenting the use of their personal information such as, right to have confirmation over what data is being held and what is being disclosed etc. [106]

There is also here a need to highlight that if the personal data is compromising of a person's status in the community then it shall provide to the "data principal" anonymity for sake of privacy. The committee also stresses that "sensitive" data such as sexual orientation, biometric data, caste and category of reservation if any; religion etc should not be

[105] Section 39 of the bill.

[106] Section 41 of the bill. The conditions listed for permitted transfers of critical personal data are in section 34(2): "any critical personal data may be transferred outside India, only where such transfer is— (a) to a person or entity engaged in the provision of health services or emergency services where such transfer is necessary for prompt action under section 12; or (b) to a country or, any entity or class of entity in a country or, to an international organisation, where the Central Government has deemed such transfer to be permissible under clause (b) of sub-section (1) and where such transfer in the opinion of the Central Government does not prejudicially affect the security and strategic interest of the State."

processed unless the "data principal" gives explicit consent which shall be dependent on the purpose of such data being collected in the first place.

This committee recommends that the data be stored in servers all across India and cross-border sharing of any "Critical personal Data" must comply with contractual clauses as may be drawn up at the time such transaction arises.[107]

This bill also makes an exception of averting consent in the case of "functions performed by the state, authorized by law", "delivering medical or health services during emergencies or epidemics, and providing services during disasters or the "breakdown of public order." It also contains exemptions from the requirements for "purposes related to employment." In addition, regulations can be made to provide exemptions from consent requirements on grounds such as "prevention and detection of unlawful activity, whistle blowing, mergers and acquisitions, credit scoring and recovery of debt." The bill also exempts kinds of data collection that are for fulfilling specific requirements such as any functions of "any agency of the government" from all or any provisions, by passing an order overriding this bill. Also, this bill stands null and void in cases the data is collected via investigative processes, legal proceedings, domestic purposes, journalistic activities, and statistical and or research purposes. [108]

This bill addresses all the concerns that were raised in the DNA Bill. Such as, the "data fiduciary" will be required to only store the data till the purpose for which it was collected is fulfilled. This bill imposes limitations on the use of the data that is collected. The consumer or the "data principal" can request that their personal data be removed or deleted

[107] Ibid.
[108] Ibid.

preventing further disclosure, to have the freedom of transferring data to another data fiduciary and to offer corrections or amendments to the stored data by way of invoking the right to be forgotten, right to data portability and right to correction and erasure respectively. This "right to be forgotten" is derived from the EU where it has been used by "data principals" to withdraw their consent from disclosure of their personal information once its necessity has been fulfilled such as people can request their unflattering and embarrassing records being taken down from websites that compromise their credibility and harm their reputation in the eyes of the public

The data fiduciaries are obligated under this bill to implement privacy safeguards, comply with transparency requirements and to create methods to protect the data stored by way of de-identifying personal data by encryption etc. It is their duty to ensure that "sensitive personal data" is completely protected under their regime and will not be subject to threats from other sources trying to gain access. For addressing this concern they are to employ "grievance redress systems" for preventing the misuse.

The proposed legislation attempts to provide for a comprehensive framework that applies to data collection and its usages whilst keeping in check with privacy, but there are various drawbacks and lacunas in the bill that are left unaddressed. Such as, the key feature kept in mind whilst framing this bill has been to protect the data principals form harmful uses of their respective data, however, the bill does not identify the specific practices that are derogatory; instead it lays immense importance to consent. The Srikrishna committee regarded these provisions as foundational to the legislation. The notice and choice framework to secure an individual's consent is the bulwark on which data processing

practices in the digital economy are founded. It is based on the philosophically significant act of an individual providing consent for certain actions pertaining to her data.[109]

The bill's consent based approach seems redundant and fails to recognize the already existing legal frameworks that have already failed to regulate consent. Securing consent as means for protection of data is pointless because of the technological advancements. The Srikrishna committee also accepts that this approach is archaic because there is a plethora of evidence to suggest that the whole process of notice and consent has become meaningless in this internet age. But the committee does not completely negate the consent based approach but adds a hue to it by saying that there needs to better consent architecture in place for protecting privacy, in a way pointing out that this bill needs to have more robust consent seeking provisions and protections. [110]

The Srikrishna committee also noted that users must contend with an overabundance, not a scarcity, of disclosure-related information about consent under existing frameworks. If current consent mechanisms lead to information overload and consent overload, the idea of "stronger" consent proposed in the bill is likely to exacerbate these issues. The proposed framework would therefore provide more information to consumers (consent agreements will have to contain more disclosures and more rights and obligations, and fresh consent will be required for a fresh purpose), without necessarily increasing data privacy.[111]

[109] Section 30 of the Bill
[110] Bart Schermer, Bart Custers, and Simone van der Hof, "The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection," Ethics and Information Technology 16, no. 2 (2014): 19, 10/06/2020 01:15 pm https://link.springer.com/article/10.1007/s10676-014-9343-8.
[111] Committee of Experts under the Chairmanship of Justice B. N. Srikrishna

Now to address some concerns regarding the Bill are under the following heads- [112]

1. **Consumer protection needs to be made priority for the bill to adequately address the data privacy**

Under Section 12, the bill provides for grounds for processing personal data without consent. Although, as mentioned before, there is no provision of "notice" to be given to the individuals in case of "non-consensual" processing of their data, which earlier existed in the 2018 Draft Bill. This creates an asymmetrical relationship between the data fiduciary and the data principal. Hence the provision of notices shouldn't be disregarded and should be included in the bill so the individual at all times has the final authority in matters relating to his data.[113]

The second inconsistency under this head is the, provision that penalizes "withdrawal of consent" by an individual. Under section 11(6), the Bill imposes liability on the data principal in the event he withdraws his consent. The provision prescribes legal consequences and a suit to be instituted in case of the withdrawal of consent. Outright it can be pointed out that there can't be consent, if it is qualified with restrictions. And this contradicts section 11 (1) (e) of the act which states that "consent should be capable of being withdrawn, having regard to whether the ease of such withdrawal is comparable to the ease with which consent may be given.". The imposition of legal consequences taints the whole process of acquiring of data. Therefore, the only plausible explanation

[112] Initial Comments of Dvara Research dated 16 January 2020 on the Personal Data Protection Bill 2019 introduced in the Lok Sabha on 11 December 2019, 10/06/2020 01:15 pm, https://www.dvara.com/research/wp-content/uploads/2020/01/Initial-Comments-on-the-Personal-Data-Protection-Bill-2019.pdf

[113] Samuelson Law, Technology & Public Policy Clinic. (2007, December). Security Breach Notification Laws: Views from Chief Security Officers, University of California, Berkeley: 10/06/2020 01:16 pm https://www.law.berkeley.edu/files/cso_study.pdf

acceptable is that the withdrawal of consent should only be met by termination of contract of services between the data principal and data fiduciary.

As mentioned earlier, the bill gives few rights to data principals. The bill should also include- right to adequate data security, rights to privacy by design (Section 22 for data fiduciary) (including privacy by default), right to breach notification, right relating to automated decision-making, right to informational privacy and right against harm.[114]

These rights to be exercised, requires the data principal to pay a fees under section 21(2). This needs a rectification to include all earning sectors of the country; therefore the fees should very minimal or shouldn't be there at all. The Bill needs to ensure the balance between the relation of data principal and data fiduciary if it truly seeks to achieve protection of data in this rapidly changing digital economy.

Under section 83(2) titled- Offences to be cognizable and non-bailable, the bill through this provision states that the data principal has no right to directly file a complaint in the court for an offence committed under this Bill. It only gives power to a court to take cognizance, *only when the complaint is filed by the DPA.* This provision violates an individual's right to seek remedy which is a right confirmed by the Supreme Court after it struck down the synonymous provision of Section 47 in the AADHAR ACT wherein the court could only take cognizance *when the complaint is filed by the UIDAI.* The Supreme Court struck down this provision on the grounds of arbitrariness; hence this section will also see the same fate when tested for arbitrariness.

[114] Srikara Prasad, An Analysis of 'Harm' defined under the draft Personal Data Protection Bill, 2018, Dvara Research, (2019, October 29) 10/06/2020 01:16 pm, https://www.dvara.com/blog/2019/10/29/an-analysis-of-harm-defined-under-the-draft-personal-data-protection-bill-2018/

2. The Data Protection Authority (DPA)'s powers and functions need to be strengthened. [115]

The draft bill 2018 had better provisions relating to the powers exercisable by the DPA but the 2019 bill has diluted these powers significantly. This can be elucidated by the Section 42(1) in which the members and Chairperson of the DPA are full-time members, and it is important that the DPA also has outside expertise and technical support staff so as to not diminish the DPA's independence and competency. The older Draft bill 2018's provision was that the Selection Committee of the DPA under Section where it mentioned the CJI or another Judge of the Supreme Court, the Cabinet Secretary and an expert appointed by the CJI and the Cabinet Secretary, but this changed in the 2019 bill and it has Secretaries of the Central Government and its Ministers only. This here is evident that the power of the DPA has been devolved and this selection committee is not appropriate because the DPA that the Bill envisions is a powerful authority with powerful functions such as starting an investigation, filing civil suits and instituting penalties etc. but this is lowering it's standards. The Selection committee cannot do without an Independent outside Expert. [116]

Under the Draft Bill of 2018, the DPA had the power to notify additional categories of "personal data" which now has been vested with the Central Government under section 15, which is another example of devolution of power of the DPA. [117]

---

[115] Christopher Carrigan, Lindsey Poole, Structuring Regulators: The Effects of Organizational Design on Regulatory Behavior and Performance (2015, June), Penn Program on Regulation. Philadelphia, Pennsylvania, United States of America. 10/06/2020 01:19 pm , https://www.law.upenn.edu/live/files/4707-carriganpoole-ppr-researchpaper062015pdf

[116] The Data Protection Bill, 2018.

[117] CGAP, Dalberg & Dvara Research. (2017, November). Privacy on the Line. Retrieved January 2020, Dvara Research, 10/06/2020 01:19 pm https://www.dvara.com/research/wp-content/uploads/2017/11/Privacy-On-The-Line.pdf

3. **The powers of the State (Central Government) should be limited to avoid arbitrariness.**[118]

As aforementioned, Section 35 of this bill empowers the Central Government to exempt any agency of Government from application of Act under the grounds of "interests of security of state" whenever it considers it necessary or expedient in the interests of sovereignty and integrity of the country, national security, friendly relations with foreign states, public order or to prevent the incitement to commit offences that jeopardize these interests. In the draft bill of 2018 the exemption was based on the grounds of "procedure established by law". But this new section empowers the government to create exemptions through executive orders which gives ample of leeway for the Government to violate personal autonomy. This bill treads on very shaky foundations and if this bill ever wishes to see the day it becomes an Act, this section is up for the test on constitutionality for sure.

The *Puttaswamy* judgment that is the prerogative of this bill gives three restrictions to be fulfilled before this bill becomes an acceptable act. These are- the action of the State must be validated by a law if it wishes to abrogate the right to privacy, secondly, is the right to liberty must be safeguarded under Article 21 therefore there should be a legitimate reason behind the state action and lastly, the test of proportionality.

The wide amplitude of powers given to the Central government under Section 35 is worrisome because it makes it difficult to determine the legitimacy and proportionality

[118] Srikara Prasad, Malvika Raghavan, Beni Chugh , & Anubhutie Singh, (2019, October). Implementing the Personal Data Protection Bill: Mapping Points of Action for Central Government and the future Data Protection Authority in India, Dvara Research Blog: 10/06/2020 01:19 pm https://www.dvara.com/blog/2019/10/03/implementing-the-personal-data-protection-bill-mapping-points-of-action-for-central-government-and-the-future-data-protection-authority-in-india/

tests both. Therefore, the draft bill's section 42(1) must be reinstated instead of this section 35. [119]

4. The provision of "sandboxes"[120]

Section 40 (4) (c) titled Sandbox for encouraging innovation etc. gives the entities in the data processing business the opportunity to experiment and create new and innovative data protection programs. Although this section means to incite creativity but it can risk the exposure of personal data to unknown risks. For this provision to work, there need to be better understanding of the nature of the data and its transactions.

5. The provisions related to the power to appropriate "anonymised data"[121]

Under sections 91(2), 91(2 B) and 91 (3) the bill talks about provisions relating to "non-personal data" to enable better targeting of delivery of services or formulation of evidence-based policies by the Central Government, in such manner as may be prescribed. The Central government under these sections have the power to direct any data fiduciary or data processor to provide any personal data anonymised or other non-personal data. This section is in stark contrast to the objective of the Bill that doesn't even mention uses of "non-personal data". The bill seeks to provide the data principal with rights over the use of their personal data hence ensuring the right to privacy. The bill, with all its provisions

[119] Malvika Raghavan, Beni Chugh, & Nishant Kumar. (2019, November). Effective Enforcement of a Data Protection Regime, 10/06/2020 01:19 pm https://www.dvara.com/research/wp-content/uploads/2019/12/Effective-Enforcement-of-a-Data-Protection-Regime.pdf

[120] UNSGSA (2019). Early Lessons on Regulatory Innovations to Enable Inclusive FinTech: Innovation Offices, Regulatory Sandboxes, and RegTech. UNSGSA, 10/06/2020 01:19 pm https://www.unsgsa.org/files/2915/5016/4448/Early_Lessons_on_Regulatory_Innovations_to_Enable_Inclusive_FinTech.pdf

[121] Srikara Prasad, Malvika Raghavan, Beni Chugh, & Anubhutei Singh, (2019, October). Implementing the Personal Data Protection Bill: Mapping Points of Action for Central Government and the future Data Protection Authority in India, Dvara Research Blog, 10/06/2020 01:19 pm https://www.dvara.com/blog/2019/10/03/implementing-the-personal-data-protection-bill-mapping-

and objectives, needs to be read altogether and not out of context. Hence, these provisions should be redacted from the Bill.

6. **The transitional provisions**

Section 97 talks about the transitional provisions. There is no time frame mentioned in the bill that states that how much time the Central Government will take to actually enact this Bill and give it the validity of an Act. There is absolute opacity as to when this data protection law will be passed in the parliament.

The Bill proposes amendments in certain laws such as- omission of 43A and Section 87 of the Information Technology Act, 2000, and amendment in Section 8 of the IT Act, 2000 and the Census Act, 1948. Bill provides minimum data protection standards for all data processing in the country. In the event of inconsistency, the standards set in the data privacy law will apply to the processing of data. The Committee recommended amendments to the Aadhaar Act, 2016 to bolster its data protection framework Section 111 and 112 of the Bill.

5.2 PROBLEMS AND LIMITATIONS OF THE BILL: A PRAGMATIC APPROACH TO PRIVACY

The aforementioned section of this chapter gives a detailed critique of the Bill. The deficiencies in this bill are that it requires more structured provisions to address the privacy concerns. Starting with the bill needs to rectify its procedure of consent and notification to the consumers for collecting their data. The problem that lies here is that while trying to maintain fair market and information practices contradicts privacy instead of protecting it. The bill also, does not prevent the users from the violation of the privacy and harms that

are caused due to it. Secondly, the wordings of the bill suggest that the bill lacks the understanding the market for information and the stakes there are for trading off this information. Srikrishna Committee did not understand what the consumers are willing to trade for the exchange of information. The bill only extends to the protection of the consumer where their privacy is infringed with evidence to show for it, and not where they are involuntarily surrendering information. Thirdly, the Bill imposes exorbitant amounts of fees on the firms that are in the business of data processing. The large scale firms suffer the most and the small firms and start ups get away with minimal fees, which results in a lot of money incurred to implement the bill. Fourthly, there are provisions of the bill that requires these data- processing business to hand over information to government agencies that fall under the "non-personal" category. It is pertinent to mention here that our information constitutes part of our property and hence this is a significant dilution of our right to property. Fifth, the power exercisable by the government to exempt certain agencies from the purposes of surveillance is outrageous on the face of it. This provision needs amendment to add checks and balance mechanism of the abuse of this power of the government. Lastly, the bill is begins with the proposition that the privacy is guaranteed and the provisions of this bill conform by it. The devil in the details here is that this supposition significantly strengthens the powers of the government for conducting bulk surveillance. The bill needs to focus on addressing the harm that can be caused to users from a breach of data privacy.

The initiative of this Bill is sound, because it is makes "consent" the centerpiece of the entire data protection regime, unlike privacy. It emphasizes that data should be processed only if prior, free, informed and specific consent has been obtained and any data processing

without the permission would result into penalties. For strengthening this purpose the bill creates a specific category of "sensitive personal data" that shall only be accessed on "explicit consent" which can only be obtained after giving the "data principal" requisite information about why their data is being collected and how it will be appropriated. Subsequently, the rights and obligations of the "data fiduciaries" are also mentioned in this Bill.[122]

One of the biggest problems with this bill is vesting the government with powers of wide amplitude to regulate business who collect data, to exempt any agency, and setting any other additional conditions or requisites for categorizing data. These powers of exemption can even validate surveillance. Currently, government surveillance has to follow the procedure prescribed under the Telegraph Act 1885 or the Information Technology Act, 2007.

CHAPTER 6

CONCLUSION AND SUGGESTION

[122] Ibid.

6.1 CONCLUSION

The aforementioned chapters have taken a course through analyzing DNA privacy, the critical analysis of the DNA Bill, the cases and circumstances that led to the landmark *Puttaswamy* judgment, the analogies and differences from an international point of view and the pros and cons for a pragmatic approach to a sustainable and durable data protection law.

The first point of inquiry about the DNA data and the DNA Bill 2019 which begets the whole discussion above is that the DNA privacy law in India is at a very nascent stage and it is very acceptable too because we didn't even have the fundamental right to privacy until very recently. So naturally the DNA Bill 2019 is very immature and poorly drafted to list the least. It lacks majorly in addressing the issues of violations of privacy and offers no to minimum safeguards. The bill also lacks in definition clause and does not afford much attention to element of "consent". The DNA Bill needs to provide clarity on the type of DNA it intends to store. It needs to afford more attention to "junk DNA" for the sake of any confusion. The storage facilities that shall hold these DNA samples should also function to a standardized procedure and should ensure that there isn't any contamination of DNA and Section 35(2) must be removed that states that the DNA samples shall be used for training purposes. It has been discussed in the previous chapters that DNA is a gold standard when it comes to forensic evidence therefore this question stands answered that the right to privacy should extend to the DNA evidence where the sole conviction depends upon it.

There is conflict of interest in the DNA Regulatory Board in its constituent members, their appointment and its adjudication. DNA is scientific piece of evidence and there is much

expertise required to understand its nature, characteristics, implications etc and hence there should be forensic scientists and experts on the DNA Regulatory Boards to facilitate the fair delivery of justice. There is very limited rights afforded to the people who's DNA shall be stored. There is little to no provision of expulsion of DNA samples from the databases once they have fulfilled their purpose. One of the biggest problems in this legislation is that it raises a presumption against the five categories of people who's DNA shall be stored by the State for the purposes of identification. The powers vested with the Central Government enables them to misappropriate this data. They can easily incarcerate any individual who's DNA profile they have stored. They can plant false evidence, can hamper reputation, can expedite cases pending against under trails and the constant extended the threat to the families of those who's DNA have been stored are also at risk. This Bill will be most fatal to the vulnerable marginalized groups of the society, as it will enable the state to brand the poorer sections and socially backward sections of the society, that are believed to have a criminal disposition. Our criminal justice system is largely in the hands and pockets of the powerful and rich of the society and is wired to discriminate against the poor, who cannot spend on their defenses and hence are at the mercy of the State machinery.

This bill has also given wide discretionary powers in the hands of the police to impound any person they have reasonable suspicion against and these powers also stem from the Code of Criminal Procedure. This bill will make the marginalized poorer sections of the society succumb to more unlawful arrests, searches and criminal prosecution.

This Bill will also prove detrimental to sex workers. Under this Bill the DNA profiles of all offenders are to be indexed. Under the Immoral Traffic (Prevention) Act, the sex

workers are categorized as offenders. It is an occupational hazard for the sex workers to be exposed to Sexually Transmitted Diseases and if this Bill indexes their DNA, they will be prejudiced against and will not be able to seek medical aid. These are only a few instances where the vulnerable and defenseless citizens suffer the consequences of this Bill and the Bill does not have a safety valve to protect these citizens that comprise a major part of our population.[123]

Therefore it is safe to conclude that the Bill gives ample powers in the hands of the State and by extension is validating state surveillance. The DNA Bill needs to redrafted, there has to be more protection afforded to the people who are surrendering their DNA samples to the state and ultimately, it all boils down to, that every effort and every endeavor must be to ensure that we don't convert our country into a police state that is plagued with the constant threat of state surveillance. The research question stands answered here that the DNA Bill 2019 does not adequately address the privacy concerns and is violating the right to privacy as upheld in *Puttaswamy.*

As far as the Data protection Bill is concerned, it is far better in its wording than the DNA bill. As per section 2 (19) which states that DNA being 'personal information' is "genetic data" under the Personal Data Protection Bill and should be protected by giving the appropriate rights to the individual who's DNA is being stored rather than the State. This bill will help supplement the DNA Bill and will provide for more rights in the hands of the data principals i.e., the people. We need to have a robust data protection regime to ensure that there is not one but two-tier safeguards to the right to privacy. The Data Protection

[123] Supra n. 8, p. 18

Bill 2019 needs amendment too, to make it more efficient. Such as that there needs to be a limitation set for the powers afforded to the Central government, the powers of the Data protection authority (DPA) needs to be strengthened, the government should refrain from appropriating any "non-personal data" etc. There are many other rights that the Data protection bill seeks to protect and give which will truly supplement the DNA bill such as the right to have data destroyed, the right to be forgotten etc. So, for the DNA Bill to be enacted it must first incorporate transparent procedures of expulsion and destruction of data by the "data principal" i.e., the people and that can only happen if there's a complimentary data protection act already in place[124], so this question stands affirmatively answered that the data protection bill should and must precede the DNA Bill. So, this question stands answered that the Personal Data Protection Bill should precede the DNA Technology (Use and Application) Technology Bill.

The above chapters discuss the stark contrast of genetic privacy legislations in other countries as compared to India. India is just beginning to recognize the need for these laws, whereas countries like USA, UK, Japan, Italy, Australia, and Germany have had DNA Databases and governing statutes and acts to supplement it since the early 60s. The advancement of the DNA technology and its use in and beyond criminal investigations can be understood very clearly from other countries. USA, UK, Japan and Germany have had very extensive nationwide DNA databases and have specific criterion for protection of privacy. Although it goes without saying that these countries are not unfamiliar with

[124] Shweta Mohandas and Elonnai Hickok, The DNA Bill has a sequence of problems that need to be resolved, The Centre for Internet and Society, Newslaundry January 14, 2019, 27/07/2020 11:52 am, https://cis-india.org/internet-governance/blog/newslaundry-elonnai-hickok-and-shweta-mohandas-january-14-2019-dna-bill-has-a-sequence-of-problems-that-need-to-be-resolved

litigations from the advocates of the right to privacy and have faced multiple challenges and still continue to do. The most important lesson that these foreign countries provide is that there needs to be a legitimate overbearing reason that outweighs the cons of the databases. Because these countries have had DNA databases for so long is the testament to the fact that they were vigilant of the right to privacy when our country was still debating over it. It is needless to say that they have also been rebuked over having DNA databases and even being accused of replicating a police state in the country. And these instances in these other countries only teach us what we can and should avoid when we frame our genetic privacy law. Therefore, the DNA bill and the Data Protection Bill need to strike a balance between the overbearing state interest and the rights of the individuals. The individual is and shall always remain at the heart of privacy.

The right to privacy has been vehemently established in the above chapter (CHAPTER 3) in the absolute mind-blowing interpretation and wisdom of the Supreme Court of India in penning down the *Puttaswamy* judgment. The bench has dealt with each and every aspect of the word "privacy" and its spirit. The 9 judges have discussed the roots and foundations of the word "privacy" and have woven it with the thread of liberty, dignity, autonomy and self-determination within the constitutional fabric. The judgment shall prove to be a valuable piece of jurisprudence for civil liberties for cases to follow. By setting the ground for upcoming legislations in the country, the judgment has frowned over the State's overbearing role over the rights of the citizens under the garb of "public interest" and "compelling state interest" that have been a concern in many cases previous to the Puttaswamy judgment. The Supreme Court reiterated the view in the *Puttaswamy* that our fundamental rights are non-derogable even for a "compelling state interest". Nothing

abrogates Part III and no "narrow tailoring" of a law can circumvent this. It can be safely said that this also extends to the right to privacy. It is the legitimate expectation from the DNA Technology (Use and Application) Bill as a legislation to be just, fair and reasonable and not be arbitrary in its purpose. The DNA Bill 2019 abrogates the rights of individuals and gives powers in the hands of the State machinery by means of "maintaining public order", "public interest" and "national security" to override the rights of the citizens, hence the hypothesis that this Bill is violative of the right to privacy under the veil of compelling state interest stands proved.

SUGGESTIONS

- There is a need for a CODIS- contemporary in India as well; this is an unquestionable need for strengthening our criminal justice system. It will help us to solve crimes so much faster and with more accuracy, this bill has the heart in the right place with its objective to identify certain categories of persons, but it needs to more intricately dealt with, more elaborated and with more privacy safeguards.
- To reach for a middle ground, the parliament has tabled the idea of having a National Registry for Sexual Offenders[125] following in the footsteps of many other countries like USA, UK, and Canada etc. These countries have had privacy challenges against their DNA databases too. It has been held by the European Court of Human Rights that this system of storing of information in a government data base is against the right to privacy of an individual. The Registry in India is veiled as an initiative to combat the growing numbers of sexual assault and rape in India.

[125] Vrinda Bhandari, Advocate Supreme Court of India, "Why India's registry of sex offenders may do more harm than good", www.scroll.in, 22/07/2020, 05:05 pm, https://scroll.in/article/895346/why-indias-registry-of-sex-offenders-may-do-more-harm-than-good

The registry shall have all the details such as the name, address, bank details, family information, PAN card number, AADHAR number, DNA samples, fingerprints and the like. The registry aims to store this personal information for certain specified time periods such as for 15 years in cases of "petty crime", 25 years for "medium level offences" and for an indefinite period of time in cases of "serious crimes such as that of the repeat offenders, rape, gang rape, sexual assault etc".

- This registry makes no distinction on the basis of age of the offender even though it should either entirely exclude juveniles or it must have a separate platform for it. Therefore the DNA database that shall function better in our country must distinguish and categorized indexing on the basis of the various offenses, the age of the offender, they punishment for the offence.
- There should be a separate database that shall exclusively deal with the Missing persons apart from the DNA database for expediting their investigations.
- The conditions in India and the realistic standard of our criminal justice system are plagued with innumerable problems. Majority of the prisoners in our jails are under-trials and to have their information stored in national databases will not prove fruitful. Our country wants to be a pinnacle as a developing democracy but we need to realize that we live in a state that has major resource and money scarcity. We live in a state of constant never-ending poverty and it is cannot venture these projects without having to think of the cost effects of it. The DNA sample collection, storage facilities, their maintenance and testing themselves will result in heavy expenditures. So, it requires a major investment from the government and

a extensive training program for the law enforcement agencies (police primarily) to actually aid criminal investigations through DNA.

- Another important concern that the National Registry should address is the "presumption of guilt" of the accused. If there is already DNA evidence against an under-trial prisoner, it is a canon in the hands of the prosecution to prove his guilt based on raising a presumption that he's a registered so he must have done it, beyond a reasonable doubt. This needs to be remedied if there ever is a National registry in our country.
- On the very first mention of having this registry seems like it might be a good thing. But it may even do more harm than good. The whole discussion in the above chapters only contend one thing and that is the right to privacy which now stands safeguarded by the Constitution. So will this serve the purpose of crime reduction, will this actually be a deterrent or will this lead to a whole new can of worms of privacy violations? Will the expansion of DNA databases lead to dispensing of "justice" in criminal cases, is a concern that needs to be addressed still.
- India can begin with having a DNA database in every state that is on the lines of a Sex Offenders Registry in the US that documents the personal information of *only* those individuals who have been incarcerated, imprisoned, served their sentence and are now released from the prison.
- This shall deter them from reoffending. The first step to a DNA database can begin with having a consolidated list of violent offenders from preventing them from re-offending. There is no need at this beginner stage to have the DNA profiles of accused persons who have not been convicted yet, arrestees, under trials etc. so

they are not being prejudiced in the eyes of the law before they have their day in court.

- The local police of that area where this registered offender resides should have access to this DNA database to know of their surroundings and neighborhoods and are informed if a person who is on the registry has moved to their locality. This does seem like branding him and subjecting him to frequent searches and seizures by the police and discrimination but the public's safety takes precedence over the reputation of an ex-convict.
- To safeguard the rights of these persons in the registry, they should be all assigned to a local police officer (not below the rank of a constable) to make routine checkups on their whereabouts and to ensure they are not a danger to themselves and to the society. This does require more man power and burdens the police more than it already is, but it can prove effective in reforming these released ex-convicts.

BIBLIOGRAPHY

Primary Sources

- The DNA Technology (Use and Application) Bill 2019
- The Personal Data Protection Bill 2019

- The Constitution of India, 1950
- The Indian Evidence Act, 1872
- The Indian Penal Code, 1860
- Fourth Amendment to the United States Constitution

Secondary Sources

Books

- M P Jain – Indian Constitutional Law Eighth Edition, 2018
- Sheldon Krimsky And Tania Simoncelli, Genetic Justice- Dna Data Banks, Criminal Investigations And Civil Liberites, Columbia University Press, New York, Isbn 978- 0- 231- 51780- 5 (Electronic) Pg- 167-212

Cases

FOREIGN JURISDISCTION

- Griswold v. Connecticut 14 L Ed 2d 510 : 381 US 479 (1965).
- Roe v. Wade 35 L Ed 2d 147 : 410 US 113 (1973).
- Grutter v. Bollinger 539 US 306, 333 (2003).
- United States v. Miller 307 U.S. 174
- Maryland v. King 133 S. Ct. 1958, 1966 (2013)
- S and Marper v. United Kingdom [2008] ECHR 1581

Articles

- Andrea Roth, Maryland v. King *and the Wonderful, Horrible DNA Revolution in Law Enforcement*, 11 OHIO ST. J. CRIM. L. *295*, 308-09 (2013)
- Arnold H. Loewy, *A Proposal for the Universal Collection of DNA*, 48 TEX. TECH L. REV. 261, 267 (2015)

- Barry Steinhardt, *Privacy and Forensic DNA Data Banks, in* DNA AND THE CRIMINAL JUSTICE SYSTEM: THE TECHNOLOGY OF JUSTICE 190 (David Lazer ed., The MIT Press 2004);
- Christina M. Gagnier, On Privacy: Liberty In The Digital Revolution, Journal Of High Technology Law, 11(2), Pp. 229-279.
- Colloquy, *Is the "JUNK"DNA Designation Bunk?, 102* NW. U. L. REv. 54,56 (2007).
- David H. Kaye, *Please, Lets Bury the Junk: The CODIS Loci and the Revelation of Private Information, 102* Nw.
- Dhiraj R Duraiswami, Privacy And Data Protection In India, Journal Of Law & Cyber Warfare, Vol. 6, No. 1, Summer 2017, P. 166-187.
- Dr. Helen Wallace, statement in the Grand Chamber of the European Court of Human Rights Between *"S" and Marper v. The United Kingdom*, application nos. 30562/04 and 30566/04.
- Gautam Bhatia, State Surveillance And The Right To Privacy In India: A Constitutional Biography, National Law School Of India Review, Vol. 26, No. 2, 2014, P. 127-158
- Hosokai (Lawyers' Association), Admissibility of Expert Evidence based on MCT 118 DNA Analysis-*Ashikaga* Case, Adjudicated on July 17, 2000 (2003), summarized and translated by E. Omura, January 2008.
- M. Dawn Herkenham, Retention of Offender DNA Samples Necessary to Ensure and Monitor Quality of Forensic DNA Efforts: Appropriate Safeguards Exist to Protect the DNA Samples from Misuse, 34 J.L. & 380, 381 (2006). MED. ETHICS

- Madison Julia Levine, Biometric Identification In India Versus The Right To Privacy: Core Constitutional Features, Defining Citizens' Interests, And The Implications Of Biometric Identification In The United States, University Of Miami Law Review, Vol. 73, No. 2, Winter 2019, P. 618-[Vi].
- Meghan J Ryan, "The Privacy, Probability, and Political Pitfalls of Universal DNA Collection" (2017) 20:1 SMU Science & Technology L Rev 3
- Natalie A Bennett, "A Privacy Review of DNA Databases" (2008) 4:3 I/S: A J of L & Policy for the Information Society 821.
- Nimisha Srinivas And Arpita Biswas, Protecting Patient Information In India: Data Privacy Law And Its Challenges, NUJS Law Review, Vol. 5, No. 3, July-September, 2012, P. 411-424
- R.E. Gaensslen, *Should Biological Evidence or DNA be Retained by Forensic Science Laboratories After Profiling? No, Except Under Narrow Legislatively-Stipulated Conditions,* 34 J. L. MED. & ETHICS 375,377 (2006).
- SAHRDC, The Ferreira Case: All That Is Wrong With Torture And Narco-Analysis, Economic And Political Weekly, Vol. 45, No. 21 (May 22-28, 2010), Pp. 13-15
- Student Advocate Committee, Transcript Of The VII Annual National Law School Of India Review Symposium: Bridging The Security-Liberty Divide, National Law School Of India Review, Vol. 26, No. 2 (2014), Pp. 169-184
- Thomas P Crocker, From Privacy To Liberty: The Fourth Amendment After Lawrence, UCLA Law Review, 57(1) (Oct 2009).

- Veena Nair, Review Of The Evidentiary Value Of DNA Evidence, Nirma University Law Journal, Vol. 7, No. 1, January 2018, P. 29-48.
- Vikram Iyengar, "Maryland v. King: The Case for Uniform, Nationwide DNA Collection and DNA Database Laws in the United States" (2014) 23:1 inf & Comm Tech L 77.
- Wareren R. Webster Jr., DNA Database Statutes And Privacy In The Information Age, Health Matrix: Journal Of Law-Medicine, 10(1), Pp. 119-140

Internet Sources

- Akhil Reed Amar, *A Search for Justice in Our Genes,* N.Y. TIMES(May 7, 2002), http://www.nytimes.com/2002/05/07/opinion/a-search-for-justice-in-our-genes.html
- Anirudh Burman, *Will India's Proposed Data Protection Law Protect Privacy and Promote Growth? The Growth of Privacy Regulation and the Bill* , Carnegie Endowment for International Peace (2020) https://www.jstor.org/stable/resrep24293.4
- Bart Schermer, Bart Custers, and Simone van der Hof, "The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection," *Ethics and Information Technology* 16, no.2 (2014): 19, https://link.springer.com/article/10.1007/s10676-014-9343-8.
- CGAP, Dalberg & Dvara Research. (2017, November). *Privacy on the Line.* Retrieved January 2020, from Dvara Research: https://www.dvara.com/research/wp-content/uploads/2017/11/Privacy-On-The-Line.pdf

- Christopher Carrigan, Lindsey Poole, Structuring Regulators: The Effects of Organizational Design on Regulatory Behavior and Performance (2015, June), Penn Program on Regulation. Philadelphia, Pennsylvania, United States of America. 10/06/2020 01:19 pm , https://www.law.upenn.edu/live/files/4707-carriganpoole-ppr-researchpaper062015pdf
- Court Rejects Retrial Request from Man Convicted of Killing Girl Through DNA, "GaijinPot.com, February 13, 2007, http://gaijinpot.com/search/index/lang/en?q=court+rejects+retrial+request
- David H. Kaye, 'Why So Contrived? The Fourth Amendment and DNA Databases after *Maryland v King'* (2014) 104 J Crim L *&* Criminology (forthcoming) http://papers.ssrn.com/sol3/papers.cfm?abstract id=2376467
- Dr. Shashi Tharoor, *Dr. Shashi Tharoor on The DNA Technology (Use and Application) Regulation Bill, 2018*, available at https://www.youtube.com/watch?v=ifO2nlY_2QY **,** last seen on 06/07/2020 10:59 pm
- Dvara Research. (2018a, February 7). *The Data Protection Bill, 2018.* Retrieved from Dvara Research: https://www.dvara.com/blog/wp-content/uploads/2018/02/Data-Protection-Bill-Draft-Dvara-Research.pdf
- Eric Posner, *The Mother of DNA Databases,* SLATE (Mar. 5, 2013), http://www.slate.com/articles/newsand-politics/view from chicago/2013/03/dna_at_ the_supreme_court_the_case_for_a_universal_database.html

- German Code of Criminal Procedure, Section 81g [DNA Analysis] (2) http:// www.iuscomp.org/gla/statutes/StPO.htm#81g
- Hermann Schmitter and Peter M. Schneider, "Legal Aspects of Forensic DNA Analysis in Germany," *Forensic Science International* 88 (1997): 95– 98, citing *Neue Juristische Wochenschrift* (NJW, translated as *New Legal Weekly*) 1990, 2944– 2945, http://rsw.beck.de/rsw/shop/default.asp?site=njw
- Initial Comments of Dvara Research dated 16 January 2020 on the Personal Data Protection Bill 2019 introduced in the Lok Sabha on 11 December 2019, Dvara Research , https://www.dvara.com/research/wp-content/uploads/2020/01/Initial-Comments-on-the-Personal-Data-Protection-Bill-2019.pdf
- J.D. Watson & F.H.C. Crick, *A Structure for Deoxyribose Nucleic Acid*, 171 NATURE 737 (1953); *The Discovery of the Double Helix, 1951-1953, U.S.* NAT' L LIB. MED., https://profiles.nlm.nih.gov/SC/Views/Exhibit/narrative/doublehelix.html
- Japan Federation of Bar Associations (JFBA), "Opinion on the National Police Agency DNA Database System http://www.nichibenren.or.jp/en/activities/statements/071221.html
- Malvika Raghavan, Beni Chugh, & Nishant Kumar. (2019, November). Effective Enforcement of a Data Protection Regime, 10/06/2020 01:19 pm https://www.dvara.com/research/wp-content/uploads/2019/12/Effective-Enforcement-of-a-Data-Protection-Regime.pdf

- Martin Kreickenbaum, "Germany: Expansion of DNA Testing— A Step Towards Genetic Registration," World Socialist Website, February 24, 2005. http://www.wsws.org/articles/2005/feb2005/dna-f24.shtml
- Robin Williams and Paul Johnson, "Inclusiveness, Eff ectiveness and Intrusiveness: Issues in Developing Uses of DNA Profi ling in Support of Criminal Investigations," *Journal of Law, Medicine and Ethics* 33, no. 3 (2005): 545– 558, quotation at 547, http:// www.ncbi.nlm.nih.gov/pmc/articles/PMC1370918/pdf/nihms-6441.pdf
- *S. and Marper v. The United Kingdom*, 30562/04 [2008] ECHR 1581 (December 4, 2008), ¶ 69, http:// www.bailii.org/eu/cases/ECHR/2008/1581.html
- Samuelson Law, Technology & Public Policy Clinic. (2007, December). *Security Breach Notification Laws: Views from Chief Security Officers.* Retrieved January 2020, from University of California, Berkeley: https://www.law.berkeley.edu/files/cso_study.pdf
- Srikara Prasad, (2019, October 29). *An Analysis of 'Harm' defined under the draft Personal Data Protection Bill, 2018*. Retrieved from Dvara Research: https://www.dvara.com/blog/2019/10/29/an-analysis-of-harm-defined-under-the-draft-personal-data-protection-bill-2018/
- Srikara Prasad, Malvika Raghavan, Beni Chugh , & Anubhutie Singh, (2019, October). Implementing the Personal Data Protection Bill: Mapping Points of Action for Central Government and the future Data Protection Authority in India, Dvara Research Blog: 10/06/2020 01:19 pm https://www.dvara.com/blog/2019/10/03/implementing-the-personal-data-

protection-bill-mapping-points-of-action-for-central-government-and-the-future-data-protection-authority-in-india/

- UNSGSA. (2019). *Early Lessons on Regulatory Innovations to Enable Inclusive FinTech: Innovation Offices, Regulatory Sandboxes, and RegTech.* Retrieved from UNSGSA: https://www.unsgsa.org/files/2915/5016/4448/Early_Lessons_on_Regulatory_Innovations_to_Enable_Inclusive_FinTech.pdf
- Vrinda Bhandari, Advocate Supreme Court Of India, "*Why India's registry of sex offenders may do more harm than good".* Scroll. In https://scroll.in/article/895346/why-indias-registry-of-sex-offenders-may-do-more-harm-than-good Accessed on 5:05 PM , 22nd July 2020