

# Social Media, Aadhaar and Right to Privacy: A Legal Study of Dependency of Public and Private Corporation on Private Data and its Impact on Right to Privacy

Rahul Raman\*

“Every man’s house is his castle”

*Globalization should be taken as access to everything at its lower price. Privacy evades definition; hence it sits uneasily with the law. Even a layman can feel like both terms have developed their roots at the opposite pole of each other. The base of this paper lies where these two polar things crossed each other and gave birth to a hot topic to be discussed by the legal fraternity. The paper basically aims to analyze the two important case pending before the Supreme court of India i.e., one related to the agreement signed by the Facebook and Whatsapp, where they agreed to share confidential information of their consumers. Secondly, the AADHAAR case which is still under discussion on the floor of the honorable court. India being a developing country and having one of the largest populations has its own problem. This paper analyses the agreement between the social media giants, its impact on the Indian subcontinent and the pending case before the Supreme Court of India. Even the researcher will try to find out the response of the developed countries and will analyze the position of Indian privacy law. After analyzing the above-mentioned problem, the research will eventually try to come up with all the possible solutions to these problems in light of the previous judgments of the Indian Supreme Court in this regard.*

## Introduction

This is the age where the best and cheapest will survive. Developing countries like India is too much indulged in the race of industrialization that the government is totally lacking the privacy and security concerns. Here the word “Globalisation” should be interpreted in widest amplitude. The economists have given some new theory of globalization. They have given importance to everything whether that would be a commodity or customers. Since the situation is changing as per the demand of time, the law must be changed accordingly. In today’s world we are totally depended on the internet and now we are living at the stage where virtual money is more in trend than real money. Using newly advance way at the internet is becoming the status symbol but the rate of awareness among the people is much lower. After demonetization it was reported that there is 110.82% growth in cyberspace<sup>1</sup> and also there is a growth in the rate of cyber-crimes in

---

\* Rahul Raman is a practicing advocate at the High Court of Judicature, Patna.

<sup>1</sup> Nitish Chandan, ‘Internet Statistics India, 2014: 100.82% Growth in Cyber Space’, 2014,

India<sup>2</sup>. It clearly means that there is a lacuna in the Indian data protection laws. This paper is nowhere written with aimed to discuss cyber-crimes; hence this discussion should be left here only.

Our discussion starts with the two most popular cases of the Indian judicial system. One is *Justice K S Puttaswamy v Union of India*<sup>3</sup> and other is the famous Facebook controversial case where Facebook and WhatsApp were sharing personal information of their users. This paper also aims to analyze the position of private rights in the era of globalization. India's privacy jurisprudence is different from the rest of the world. Due to the remarkable position of ours that India is a "developing country", we are struggling a lot when it comes to competing with the developed countries. But the trading giants of every field are from a developed country. Furthermore, it will analyze the situation that whether the law should also be implemented globally or it should be implemented in light of the local situation. Here the effectiveness of India's data protection laws will be tested w.r.t. the features of globalization.

Privacy evades definition and for this reason, sits uneasily with the law. Privacy is the tool through which an individual conditioned its relationship with the rest of society. The multiplicity of everyday privacy claims and transgressions by ordinary people, and the diversity of situations in which these occur confuse any attempt to create a common meaning of privacy to inform law.<sup>4</sup> The article is geared towards a realist conception of privacy rights and does not posit them in an overly broad or moralistic hue.

### Privacy Jurisprudence in India

The Greek philosopher Aristotle spoke of a division between the public sphere of political affairs (which he termed the polis) and the personal sphere of human life (termed oikos). This dichotomy may provide early recognition of "a confidential zone on behalf of the citizen".<sup>5</sup> Aristotle's distinction between

---

*The Cyber Blog India Official Website* available at <http://www.cyberblogindia.in/internet-statistics-india-2014-100-82-increase-users-cyber-space-needs/>, accessed on 11 January 2018.

<sup>2</sup> Siddharth Tadepalli, 'Cyber-crime cases shoot up post demonetization', *The Times of India* (2016) available at <http://timesofindia.indiatimes.com/city/hyderabad/Cyber-crime-cases-shoot-up-post-demonetisation/articleshow/56129277.cms>, accessed on 11 January 2018.

<sup>3</sup> *Justice K S Puttaswamy v Union of India*, Writ Petition (Civil) no 494, 2012.

<sup>4</sup> Bhairav Acharya, 'Privacy Law in India: A Muddled Field', 2014, *The Hott Official Website* available at <http://www.thehoot.org/free-speech/privacy/privacy-law-in-india-a-muddled-field-i-8722>, accessed on 2 February 2018.

<sup>5</sup> Michael C. James, 'A Comparative Analysis of the Right to Privacy in the United States', vol. 29, *CJIL*, 1983.

the public and private realms can be regarded as providing a basis for restricting governmental authority to activities falling within the public realm. On the other hand, activities in the private realm are more appropriately reserved for “private reflection, familial relations, and self-determination”.<sup>6</sup>

Right to privacy is given utmost importance in India; hence it has been accepted as a part of Fundamental rights in Indian constitution through judicial interpretation<sup>7</sup> and this is what Indian judiciary is known for. Our judicial system has played a tremendous role in creating something which is not in the system for the betterment of the public. India has had a strong tradition of civil society/NGO/Trade Union participation in demanding political accountability and NGOs have been active in pressing for change in all spheres –social, legal, economic and political.<sup>8</sup> With booming e-commerce, it won't be wrong to say that “privacy” of individuals is not just about their privacy at home but shall be applied in a much wider sense, including privacy of voice conversations, property, bank account, health records, passwords, photographs, business ideas, electronically transmitted communication etc.. This right, first enunciated by Samuel D Warren and Louis Brandeis in the Harvard Law Review in 1890<sup>9</sup>, has been examined by the Supreme Court of India time and again<sup>10</sup>. The law of privacy is recognition of the individual's right to be let alone and to have his personal space inviolate. It is the product of an increasingly individualistic society in which the focus has shifted from society to the individual. The technology which provided a justification for the need to preserve the privacy of an individual was the development of photography. At that time Dean Roscoe Pound observed and said that the invention of this new right has added a new chapter to the legal theory. A citizen has a right “to safeguard the privacy of his own, his family, marriage, procreation, motherhood, childbearing and education among other matters.”<sup>11</sup> In the series of cases like *Gobind v State of Madhya Pradesh*<sup>12</sup> and *People's Union for Civil Liberties v Union of India*<sup>13</sup>, the Honourable Supreme Court of India has advocated for the right to privacy as a fundamental right. The reasoning was very much accepted as the right to privacy is not something new

---

<sup>6</sup> Ibid, p. 26.

<sup>7</sup> *Justice K S Puttuswamy and Anr. V. Union of India and Ors.* (n 3).

<sup>8</sup> Report of The Centre for Internet Society, *Privacy in India*, The Country Report, October 2011 available at <http://cis-india.org/internet-governance/country-report.pdf>, accessed on 2 February 2018.

<sup>9</sup> Warren & Brandeis, ‘The Right to Privacy’, vol. 5, HLR p. 2, 1890.

<sup>10</sup> Varun Marwah, ‘Can I have some privacy, please?’, 2016, Bar and Bench available at <https://barandbench.com/can-privacy-please/>, accessed on 2 February 2018.

<sup>11</sup> MP Jain, *Indian Constitutional Law*, 6<sup>th</sup> edition, LexisNexis Butterworths Wadhwa, Nagpur, 2011, p. 1237.

<sup>12</sup> *Gobind v State of Madhya Pradesh*, SCC, 1975, SC, p.148.

<sup>13</sup> *People's Union for Civil Liberties v Union of India*, SCC, 1997, SC, p. 301.

which is purely noble but it was present with some other term i.e., 'Right to be let alone'. 'Right to be let alone' is an integral part of 'Right to enjoy life' which is again fully acceptable as a part and parcel of 'Right to life'. In early times, the law afforded protection only against physical interference with a person or his property. Initially, this right was developed to fill the lacuna between the defamation and something which is not defamatory but still harms the reputation (and that neither be categorized as a crime nor can be said to be civil wrong).

As civilization progressed, the personal, intellectual and spiritual facets of the human personality gained recognition and the scope of the law expanded to give protection to these needs.<sup>14</sup> Since the last few years, there has been increasing traction in the field of data generation and processing, its storage and transfer and the pace at which incidents of data theft and intrusive surveillance are coming to limelight. Global corporations such as *Google, Facebook, and Amazon* whose business model is based on the collection, storage, and usage of customer data often land their customers in a vulnerable situation wherein their personal information gets commoditized by various other websites. With the internet becoming all-pervasive, there is a need to regulate the dealing of vast information stored therein and protect an individual's privacy.

In order to effectively address the privacy issues, the Planning Commission of India had directed the constitution of a 'Group of Experts' on December 26, 2011, to identify the privacy issues and prepare a report on the same to facilitate authoring of privacy bill for India. The Group was constituted under the Chairmanship of Justice A.P. Shah, Former Chief Justice, and High Court of Delhi with 11 other members (hereinafter referred to as the "Shah Committee")<sup>15</sup>. The Internet has brought new concerns about privacy in an age where computers can permanently store records of everything: "where every online photo, status update, twitter post and blog entry by and about us can be stored forever," writes law professor and author Jeffrey Rosen<sup>16</sup>. One of the most shocking but accurate information is that there is more money flowing in the cyber market as it is used in the hard form. The ability to do online inquiries about individuals has expanded dramatically over the last decade. Facebook for example, as of July 2010, was the largest social-networking site, with nearly 500 million members, or 22 percent of all Internet users, who upload over 25 billion pieces of content

<sup>14</sup> Adv. Shyam Sahu, 'Right to Privacy in India: Recent Trend,' 2013, Blogspot, available at [http://snsah.blogspot.in/2013/03/by-adv\\_23.html](http://snsah.blogspot.in/2013/03/by-adv_23.html), accessed on 3 February 2018.

<sup>15</sup> Arjun Uppal, 'Right to Privacy in India', ILJ, 2014 available at <http://www.indialawjournal.org/archives/volume7/issue-2/article3.html>, accessed on 28 March 2018.

<sup>16</sup> Jeffrey Rosen, 'The Web Means the End of Forgetting', *The New York Times* (21 June 2011) available at [http://www.nytimes.com/2010/07/25/magazine/25privacy2.html?\\_r=3&ref=technology&](http://www.nytimes.com/2010/07/25/magazine/25privacy2.html?_r=3&ref=technology&), accessed on 28 March 2018.

each month<sup>17</sup>. Twitter has more than 100 million registered users. The Library of Congress recently announced that it will be acquiring — and permanently storing — the entire archive of public Twitter posts since 2006, reports Rosen<sup>18</sup>.

The Supreme Court in *People's Union for Civil Liberties v. Union of India*<sup>19</sup> held that “We have, therefore, no hesitation in holding that right to privacy is a part of the right to ‘life’ and ‘personal liberty’ enshrined under Article 21 of the Constitution. Once the facts in a given case constitute a right to privacy, Article 21 is attracted. The said right cannot be curtailed ‘except according to procedure established by law.’” Again, the Apex Court in the case of *Ram Jhethmalani and Ors. V. Union of India and Ors.*<sup>20</sup> through the ration of the case the apex court observed that “Right to privacy is an integral part of the right to life, a cherished constitutional value and it is important that human beings be allowed domains of freedom that are free of public scrutiny unless they act in an unlawful manner.” In all the above-cited case it is widely accepted that the right to privacy is an integral part of Indian constitution. At the same time, the government has proposed a bill known as Right to privacy bill, 2011 which aimed to provide protection to individuals in case their privacy is breached through unlawful means. Even Justice B. P. Jeevan Reddy observed in the case of *R. Rajagopal v State of Tamil Nadu*<sup>21</sup> that “The right to privacy is implicit in the right to life and liberty guaranteed to the citizens of this country by Article 21. A citizen has a right to safeguard the privacy of his home, his family, marriage, procreation, motherhood, child-bearing and education among other matters. None can publish anything concerning the above matters without his consent whether truthful or otherwise and whether laudatory or critical. If he does so, he would be violating the right to privacy of the person concerned and would be liable in an action for damages. Position may, however, be different, if a person voluntarily thrusts himself into controversy or voluntarily invites or raises a controversy.”<sup>22</sup>

The Information Technology Act which came into force in the year 2000 and is the only Act to date which covers the key issues of data protection, albeit not every matter. In fact, the Information Technology Act, 2000 enacted by the Indian

---

<sup>17</sup> The U.S. Chamber of Commerce Foundation, ‘The Millennial Generation Research Review’, 12 November 2012, *U.S. Chamber of Commerce Foundation Official Website* available at <https://www.uschamberfoundation.org/reports/millennial-generation-research-review>, accessed on 29 March 2017.

<sup>18</sup> Gregg Keizer, ‘Apple denies tracking iPhone users, but promises changes’, 2011, *Computer World Official Website* available at <http://www.computerworld.com/article/2506250/data-privacy/apple-denies-tracking-iphone-users--but-promises-changes.html>, accessed on 29 March 2017.

<sup>19</sup> *People's Union for Civil Liberties v. Union of India* (n 13).

<sup>20</sup> *Ram Jhethmalani and Ors. V. Union of India and Ors*, SCC, 2011, SC, p.1.

<sup>21</sup> *R. Rajagopal v State of Tamil Nadu*, SCC, 1994, SCC, p. 632.

<sup>22</sup> *Ibid.*

Parliament is the first legislation, which contains provisions on data protection<sup>23</sup>. But there are lacunas in the said Act as it nowhere provides for the definition of personal data etc. The said act has provisions against the theft of data but it nowhere talks about the solution to the problem. In the current scenario, we have witnessed many times that our data is getting leaked and we have no idea about the thief. The said Act of 2009, nowhere talks about the current global problem but it is basically a piece of a legal document based on traditional happenings.

It is the work of legal genius that we have a right known as Right to privacy. In India, this right is not a positive right. Data protection and privacy have been dealt with in the Information Technology Act, 2000 but not in an exhaustive manner. The IT Act needs to establish a set of specific standards relating to the methods and purpose of assimilation of the right to privacy and personal data. We may conclude by saying that the IT Act is facing the problem of protection of data and separate legislation is much needed for data protection striking an effective balance between personal liberties and privacy.<sup>24</sup>

### **Right to Privacy, Data Protection, and Social Media**

In recent years if someone had really grown up then it is a social media platform. From a teenager to a giant monster or whatever you say, suit its characteristics. The then India's information and broadcasting minister Manish Tewari remarked: "Never before in the history of mankind has there been so much power in the hands of so many people and located at so many places. There's more digital content churned out every two days than that created from the beginning of civilization<sup>25</sup>."

The innovative idea of Mark Zuckerberg which is popularly known as Facebook started a revolution in this platform and added everyone with this digital world. This platform played an important role in the formation of the government of the world's two best countries i.e., the United States of America and India. If one is not using these platforms, no matter how smart he is, this *e*-generation recognizes them as a technologically challenged person. Rather than define the term using a bunch of boring jargon that would probably only complicate things further, perhaps the best way to get a clearer understanding of it is to break it down into simpler terms. To start, let's look at each word individually.

*The "social" part* refers to interacting with other people by sharing information

<sup>23</sup> Dr. Shiv Shankar Singh, 'Privacy and Data protection in India', 2012, PL February S-2.

<sup>24</sup> Gregg Keizer (n 18).

<sup>25</sup> Ardi Kolah, Rajesh Babu and Suren Sista, 'Social media and the law in India', 2013, *Indian Inc. Official Website* available at <http://www.indiaincorporated.com/item/2950-social-media-and-the-law-in-india.html>, accessed on 29 March 2018.

with them and receiving information from them. The “media” part: refers to an instrument of communication, like the internet (while TV, radio, and newspapers are examples of more traditional forms of media).<sup>26</sup> Hence, by combining the above meanings we can elaborate that *Social media are web-based communication tools that enable people to interact with each other by both sharing and consuming information*. In current tradition these social sites are used for unsocial work like murder, cheating and especially some of the terrorist organization are using this platform to spread their motto. These platforms have developed themselves in such a manner that one can do multitasking on it and without any cost. Since our concern is privacy issue hence we will not deal with the matters of E-crime. Now our concern is regarding the protection of our email and phones as they are the two things which contain every short of private information of an individual. The two giant of the digital world when merged it became a monster. They are occupying almost 85% of the total digital conversation either it may be some type of regular conversation or maybe some type of confidential corporate conversation. Facebook basically was getting its revenue from the advertisement. For advertisement, one needs to know the market and its market was not limited to some kind of small space but it is working on that space which cannot be measured. Then both merged. This concern rises with the case of *Karmanya Singh Sareen and Ors. v. Union of India and Ors*<sup>27</sup>, which came as a writ in Delhi High court questioning an agreement signed between the Facebook Inc. and WhatsApp. The facts of the case are:

“WhatsApp” was acquired in the year 2014 by Respondent No.3/”Facebook Inc.”. It is alleged that after “WhatsApp” was acquired, a drastic change has been proposed to be made in the privacy policy of “WhatsApp” and users were put on notice in August 2016. Users were asked to agree to terms and privacy policy by 25th September 2016 to continue using “WhatsApp”.<sup>28</sup> The official agreement states that:

*... ‘We plan to share some information with Facebook and the Facebook family of companies that will allow us to coordinate more, such as to fight spam and abuse, and improve experiences across our services and those of Facebook and the Facebook family. For example, once you have accepted our updated Terms and Privacy Policy, we will share some of your account information with Facebook and the Facebook family*

<sup>26</sup> Daniel Nations, ‘What Is Social Media? Explaining the Big Trend’, 2017, *Life Wire Official Website* available at <https://www.lifewire.com/what-is-social-media-explaining-the-big-trend-3486616>, accessed on 29 March 2017.

<sup>27</sup> *Karmanya Singh Sareen and Ors. v. Union of India and Ors* (MANU/DE/2607/2016).

<sup>28</sup> *Ibid.*

*of companies, like the phone number you verified when you registered with WhatsApp, as well as the last time you used our service.*<sup>29</sup>

Initially, this case was in the High Court of Judicature, Delhi where it was heard by the bench, headed by the Chief Justice G. Rohini. WhatsApp's new privacy policy allows it to collect and share information of its users' with Facebook and all its group companies for the purpose of commercial advertising and marketing on its platform.<sup>30</sup> This was challenged by the two students Karmanya Singh Sareen and Shreya Sethi on the basis of "violation of fundamental rights of users" by sharing confidential information under the privacy policy. The issue was raised in Europe also when the Hamburg Commissioner for Data Protection and Freedom of Information has ordered the social networking giant to delete all data that it has already received after terming its current practices aimed at misleading the public, an infringement of its data protection law.<sup>31</sup> The Delhi High Court ordered WhatsApp to delete users' data completely from its servers and refrain from sharing users' data with Facebook, provided that the users requested the deletion of their WhatsApp account before 25<sup>th</sup> September 2016, the date on which the users were asked to agree to the new terms, and also prohibited WhatsApp from sharing existing users' data dated before 25 September 2016.<sup>32</sup> The Court even asked the Telecom Regulatory Authority of India to decide whether such messaging platforms should be regulated, adding another dimension to the on-going debate on this subject. After the judgment of the Delhi High Court, the matter went as an appeal to the Supreme Court of India as the appellant was not satisfied by the verdict of the Delhi High Court. Harsih Salve, a Senior Advocate, argued on the behalf of the petitioner and he contended that the policy that is formulated by WhatsApp is unconscionable and is unacceptable and also suffers from constitutional vulnerability since it maladroitly affects the freedom which is a cherished right of an individual under the Constitution. By the above contention, Mr. Salve argued that the matter must

---

<sup>29</sup> Shrutti Dhapola, 'WhatsApp's privacy policy is bigger than just sharing info with Facebook', *The Indian Express*, (29 August 2016) available at <http://indianexpress.com/article/technology/opinion-technology/whatsapps-new-privacy-policy-goes-beyond-sharing-info-with-facebook/>, accessed on 29 March 2018.

<sup>30</sup> Priyanka Mittal, 'WhatsApp can't share India user data before 25 Sept with Facebook, says court', *Live mint* (2016) available at <http://www.livemint.com/Consumer/Eb4gGUsP4ZAHPRVruqZPhL/WhatsApps-can-enforce-new-privacy-policy-from-25-Sept-Delh.html> accessed on 29 March 2018.

<sup>31</sup> Indu Bhan, 'Facebook, Whatsapp case: Put privacy policies under legal framework', *The Financial Express* (20 September 2016) available at <http://www.financialexpress.com/opinion/facebook-whatsapp-case-put-privacy-policies-under-legal-framework/398488/>, accessed on 29 March 2018. 29/03/2018.

<sup>32</sup> Ninxin Xie, 'India: High Court issues "strong judgment" in WhatsApp case', *Data Guidance* (2016) available at <http://www.dataguidance.com/india-high-court-case-whatsapp-strong-judgment/>, accessed on 29 March 2018.

be heard before the constitutional bench. Now, the case is pending before the constitutional bench of Apex Court. The matter is yet not decided and we cannot deny the possibility that WhatsApp may share the personal information of its Indian users with Facebook, third parties or scamsters<sup>33</sup>. And this is our concern, we are lacking an authority to govern this, don't we have the right to keep our private messages private. This controversial deal between the two Tech giants has been banned by the European countries like Germany. This was done just after two months and in our country, the case is still pending. This is our main concern that there should be fast delivery of justice and we are in an urgent need of an authority to look into these matters. As per the report, the FTC's Bureau of Consumer Protection sent a stern letter to the companies warning them to honor their promises to consumers or face an investigation into unfair trade practices. That letter also pointed to specific pledges from the companies including one by *Facebook* CEO Mark Zuckerberg who insisted that "We are absolutely not going to change plans around *WhatsApp* and the way it uses user data."<sup>34</sup>

Even the developed countries like the United States, the United Kingdom, and European countries have opposed such types of agreement and taken it as a breach to the right to privacy of an individual. The first common law regarding the Right to privacy is *Semayne's Case*<sup>35</sup>. There has been a transformation in this approach after the Human Rights Act, 1998 (HRA) came into force. For the first time, privacy was incorporated as a right under the British law<sup>36</sup>. In *Campbell v MGN Ltd*<sup>37</sup> which is the best-suited case for the changing scenario of the United Kingdom. The House of Lords held that the applicant had a reasonable expectation of privacy. *R v The Commissioner of Police of Metropolis*<sup>38</sup> was a

<sup>33</sup> Aarthio S. Anand, 'Why the Supreme Court Shouldn't Allow WhatsApp to Share Data with Facebook', *The Wire* (2017) available at <https://thewire.in/120714/chief-justice-khehar-shouldnt-allow-whatsapp-share-indian-user-data-facebook/>, accessed on 29 March 2018.

<sup>34</sup> Jeff John Roberts, 'Facebook Plan for WhatsApp Data Poses Legal Risks', *Fortune* 500 (2016) available at <http://fortune.com/2016/08/25/facebook-whatsapp-ftc/>, accessed on 29 March 2018.

<sup>35</sup> *Peter Semayne v Richard Gresham*, 77 ER 19.

<sup>36</sup> The UK Human Rights Act incorporates the rights set out in the European Convention on Human Rights (ECHR) into domestic British law. The Preamble of the Act states that it "gives further effect to rights and freedoms guaranteed" under the ECHR. Under the Act (S. 6), it is unlawful for any public authority, including a court or tribunal at any level, to act in a manner which is incompatible with a Convention right. The Convention rights take precedence over rules of common law or equity, and over most subordinate legislation. The Act, thereby, protects the right to privacy, which has been provided under Article 8 (1) of the ECHR. See Ben Emmerson et al. (ed), *Human Rights and Criminal Justice*, Sweet & Maxwell, 2000; See also 'Concerns and Ideas about the Developing English Law of Privacy', Institute of Global Law, available at [http://www.ucl.ac.uk/laws/global\\_law/publications/institute/docs/privacy\\_100804.pdf](http://www.ucl.ac.uk/laws/global_law/publications/institute/docs/privacy_100804.pdf), accessed on 29 March 2018.

<sup>37</sup> *Campbell v MGN Ltd* [2004] UKHL, p. 22.

<sup>38</sup> *R v The Commissioner of Police of Metropolis* [2011] UKSC, p. 21.

case concerning the extent of the police's power (under guidelines issued by the Association of Chief Police Officers- the ACPO guidelines) to indefinitely retain biometric data associated with individuals who are no longer suspected of a criminal offense. The UK Supreme Court, by a majority, held that the police force's policy of retaining DNA evidence in the absence of 'exceptional circumstances' was unlawful and a violation of Article 8 of the European Convention on Human Rights.

The Constitution of the United States does not contain any specific provision related to the Right to privacy. But as we are very much aware of the judge's role in establishing a balanced constitution through judicial activism, the provided space for the Right to privacy in the United States Constitution. It starts with *Body v United States*<sup>39</sup> where the question raised before the United States Supreme Court that "compulsory production of a person's private papers to be used in evidence against him in a judicial proceeding, is an unreasonable search and seizure within the meaning of the Fourth Amendment." The Court of the United States has invalidated a state law prohibiting the possession, sale, and distribution of contraceptives to married couples, for the reason that the law violated the right to marital privacy.<sup>40</sup> *Techcrunch* a renowned website of the United States writes "Facebook is in the business of monetizing usage via interest-based advertising fed by harvesting the personal data of its users. *WhatsApp's* original business model, of charging users a small yearly subscription fee for an ad-free messaging service, was discontinued after *Facebook* took over ownership of the service."<sup>41</sup>

Now let us shift our discussion to the famous case of *Justice K S Puttuswamy (Retd) v Union of India*<sup>42</sup>. The bench has overruled its decisions in *M.P. Sharma v Satish Chandra, District Magistrate, Delhi (1954)*<sup>43</sup>, rendered by a bench of eight judges and, in *Kharak Singh v State of Uttar Pradesh*<sup>44</sup>(1962), rendered by a bench of six judges, which contained observations that the Indian constitution does not specifically protect the right to privacy.<sup>45</sup> Hon'ble Mr. Justice D.Y. Chandrachud delivered the majority judgments on behalf of his fellow judges and held that "privacy is intrinsic to life, liberty, freedom, and dignity and therefore, is an

<sup>39</sup> *Body v United States*, US, vol. 116, p. 616 (SC 1886).

<sup>40</sup> *Griswold v Connecticut*, US, vol 381, p. 479 (SC 1965).

<sup>41</sup> Natasha Thomas, 'WhatsApp to share user data with Facebook for ad targeting — here's how to opt out', *Techcrunch* (2016) available at <https://techcrunch.com/2016/08/25/whatsapp-to-share-user-data-with-facebook-for-ad-targeting-heres-how-to-opt-out/>, accessed on 30 March 2018.

<sup>42</sup> *Justice K S Puttuswamy (Retd) v Union of India*, Writ Petition (Civil) no 494 of 2012.

<sup>43</sup> *M.P. Sharma v Satish Chandra, District Magistrate, Delhi, SCR, 1954*, p.1077.

<sup>44</sup> *Kharak Singh v State of Uttar Pradesh, SCR, 1964*, p. 332.

<sup>45</sup> Anurag Bhaskar, 'Key Highlights of Justice Chandrachud's Judgment in the Right to Privacy Case', *The Wire* (2017) available at <https://thewire.in/171325/justice-chandrachud-judgment-right-to-privacy/>, accessed on 20 March 2018.

inalienable natural right". The content of the constitutional right to privacy and its limitations have proceeded on a case to case basis, each precedent seeking to build upon and follow the previous formulations. The doctrinal foundation essentially rests upon the trilogy of *M P Sharma*<sup>46</sup>– *Kharak Singh*<sup>47</sup>– *Gobind*<sup>48</sup> upon which subsequent decisions including those in *Rajagopal*<sup>49</sup>, *PUCL*<sup>50</sup>, *Canara Bank*<sup>51</sup>, *Selvi*<sup>52</sup> and *NALSA*<sup>53</sup> have contributed. Reconsideration of the doctrinal basis cannot be complete without evaluating what the trilogy of cases has decided. Even recording of a conversation between the husband and wife without his/her knowledge would amount to the infringement of their privacy as stated in *Rayala M. Bhuvaneshwari v. Nagaphanender Rayala*.

In multiple orders from 2010-2015, the Supreme Court repeatedly held it was not striking down Aadhaar as unconstitutional based on the government assurance that participation in the program was voluntary (and not mandatory). But Hon'ble Chief Justice J.S. Khehar has markedly departed from this position. On February 7, Chief Justice Khehar (along with his brother judge Justice N. V. Ramana) tacitly approved the idea of linking all mobile phones (via the SIM cards) to the owners' Aadhaar cards in the interest of national security (because it was feared unverified mobile numbers could be used for terrorist and criminal activity).<sup>54</sup> Although, the question is continuously rising on the Aadhaar that this mass surveillance technology is hampering the right to privacy of an individual. One thing must be clarified here that we the people of India full faith in the principle of the nation first. But we should not be cheated in the name of our nation. Recently we have witnessed that all the details of the famous Indian player and former skipper of the Indian Cricket team were made leaked.<sup>55</sup> The current situation of the Indian judicial system is that the constitutional bench of our apex court with the majority has accepted that Right to privacy is the part of Article 21 and hence should be accepted as the fundamental right to the citizen of India. India has Information Technology Act, 2000 which is based on the Resolution A/RES/51/162 adopted by the General Assembly of the United Nations on 30th

<sup>46</sup> *M.P. Sharma v Satish Chandra, District Magistrate, Delhi*, (n 43)

<sup>47</sup> *Kharak Singh v State of Uttar Pradesh*, (n 44).

<sup>48</sup> *Singh v State of MP and Anr.*, (n 12).

<sup>49</sup> *R. Rajgopal v State of Tamil Nadu*, (n 21).

<sup>50</sup> *People's Union for Civil Liberties v. Union of India*, (n 13).

<sup>51</sup> *Canara Bank v C S Shyam*, Civil Appeal No 22, 2009.

<sup>52</sup> *Smt. Selvi v State of Karnataka*, SCC, 2010, SC, p.263

<sup>53</sup> *National Legal Service Authority of Union of India*, Writ Petition (civil) no.604, 2013.

<sup>54</sup> *Rayala M. Bhuvaneshwari v. Nagaphanender Rayala*, AIR, 2008, AP, p. 98.

<sup>55</sup> 'MS Dhoni's Aadhaar details leaked, wife Sakshi complains to Ravi Shankar Prasad', *The Hindustan Times* (29 March 2017) available at <http://www.hindustantimes.com/cricket/ms-dhoni-s-personal-info-from-aadhar-card-form-leaked-wife-sakshi-complains/story-8M4B7ZabHIu8cAcWhKuIzH.html>, accessed on 30 March 2018.

January 1997 regarding the Model Law on Electronic Commerce earlier adopted by the United Nations Commission on International Trade Law (UNCITRAL) in its twenty-ninth session. Section 72, of the said Act, talks about the punishment for the breach of confidentiality and privacy which prescribes for the punishment of 3 years or fine up to five lakh rupees or both. Under Section 43A of the (Indian) Information Technology Act, 2000, a body corporate who is possessing, dealing or handling any sensitive personal data or information, and is negligent in implementing and maintaining reasonable security practices resulting in wrongful loss or wrongful gain to any person, then such body corporate may be held liable to pay damages to the person so affected. It is important to note that there is no upper limit specified for the compensation that can be claimed by the affected party in such circumstances.<sup>56</sup> A comprehensive analysis of precedent has been necessary because it indicates the manner in which the debate on the existence of a constitutional right to privacy has progressed. The Indian Supreme Court in *Justice K Puttuswamy (Retd) v Union of India*<sup>57</sup> in fact, overruled its observation in *Suresh Kumar Kaushal v Naz Foundation*<sup>58</sup> and observed that this court at fault while harmonizing the Article 21 of UDHR and Article 17 of ICCPR with Article 21 of the Indian Constitution and also observed that the reason stated in paragraph 48 of the *Kaushal*<sup>59</sup> the case is not a valid point to be taken into consideration.

## Conclusion and Suggestions

A constitutional democracy can survive when citizens have an undiluted assurance that the rule of law will protect their rights and liberties against any invasion by the state and that judicial remedy would be available to ask searching questions and expect answers when a citizen has been deprived of these, most precious rights. The answer is not affirmative, in the light of public policy, and transparency. Although there are various amendments and judicial pronouncements to strengthen data protection, still the existing law is not competent to cope with emerging technologies. Issues like the conflict of jurisdiction, IPR protection, domain names, still need to be addressed and the training to investigations agencies is also an important part. The researcher has witnessed an interesting case where a CD was being seized by police personnel for evidence, and to preserve the CD the Investigation Officer made a hole in it

<sup>56</sup> Vijay Pal Dalmia, 'India: Data Protection Laws in India', (2011) *Mondaq Official Website* available at <http://www.mondaq.com/india/x/133160/Privacy/Data+Protection+Laws+In+India>, accessed on 30 March 2017.

<sup>57</sup> *Suresh Kumar Kaushal v Naz Foundation*, SCC, 2014, SC, p. 1.

<sup>58</sup> *Ibid.*

<sup>59</sup> *Ibid.*

and then tagged it into the file, before producing in the court of law.<sup>60</sup>

Leaving the idea of awareness about data security and coming to the point that this data security is an issue now to win an election. This paper is nowhere aimed to raise controversy but now we are witnessing that the two major political parties of our country are making data security an issue in their election. When this research was being done the Hon'ble Supreme Court was also busy in analyzing the position of Aadhaar and data security in this country. This is a positive hope in reference to the data protection system of India and this debate between these parties will make aware the basic population of this country. Recently Facebook CEO was alleged in a popularly known as 'Cambridge Analytical Data Scandal'. Now it is very much clear that our saved data on social networking sites are being used for some other purposes and there are agencies specialized in this field. Although the CEO of the Tech giants has accepted that our data is fully safe but do we have any authority to cross-check this. The answer to this sort of question is always in a negative way because our lawmakers do not really care about our privacy. Now we have evolved so much globally that in few thousand of rupees one can buy millions of data. The report of the ministry says that the government of India has constituted a committee under the chairmanship of B.N Srikrishna to study the status of Data protection in the country and the need for Data protection bill.<sup>61</sup> We are so late that when our data got leaked, in fact, it is sold with some considerable amount and now our government has started their routine work which will take few years to make a law on that.

Based upon these illustrations we can divide India into two parts- one is full of those boys and girls who can beat anyone in technology whereas the second group comprises that personnel from rural India who rarely knows the basic usage of technology. But the question is, using the technological means that we are aware of, in every possible aspect, using social networking websites, buying/ selling and doing online trade nowhere makes us a Netizen. In fact, the pros and cons of these types of trades are rarely understood by the majority of the people of Indian. The government has indicated that it will be exploring some sort of regulations to protect the data privacy of consumers in India. A PTI report quoted Additional Solicitor General (ASG) Tushar Mehta as saying, "We are coming out with a regulatory regime on data protection. Freedom of choice

---

<sup>60</sup> Navin Shelar, 'Indian Laws on Privacy of Digital Information of Users', (2014) *I AM WIRE Official Website* available at <http://www.iamwire.com/2014/08/indian-laws-privacy-digital-information-users/84277>, accessed on 30 March 2018.

<sup>61</sup> Ministry of Electronic and Information Technology, Government of India, 'White Paper on Data Protection framework for India', (2018), *Ministry of Electronic and Information Technology Official Website* available at <http://meity.gov.in/white-paper-data-protection-framework-india-public-comments-invited>, accessed on 30 March 2017.

needs to be protected and there cannot be any doubt over it.”<sup>62</sup> But I think the process should be started at the ground level. We are entering into the cyber world and our dreams are coming true. Now it is the duty of the government to make people aware of the pros and cons of these things. In my recent research, I saw that there is a very basic difference in process of verifying the AADHAAR data between the telecom companies and public sector banks. The telecom sectors are using process authorized by UIDAI but the process developed by banking companies are not verified by UIDAI. The telecom companies don't provide a platform to access into user's personal data whereas banks can easily get user's data and there is no guarantee of the security. The researcher's basic allegation is that why the Government of India is building a parallel platform to verify AADHAAR although we have a specialized authority in this field? I think government, private and public body should be honest to the citizen of this country. There should not be any concurrent view in accepting that lawmakers of India have tried best to cover the data protection laws and in doing so they have attempted to adopt ideas from jurisdictions which have long-standing and mature data protection regulations. But this step is not an ultimate solution; in fact, it should be taken a first step towards solving the puzzle.

Upon the footprints of the foreign laws, this bill has been introduced in the Rajya Sabha known as The Personal Data (Protection) Bill, 2013. The purpose of this bill is to provide protection of personal data and information of an individual collected for a particular purpose by one organization, and to prevent its usage by other organization for commercial or other purposes and entitle the individual to claim compensation or damages due to disclosure of personal data or information of any individual without his consent and for matters connected with the Act or incidental to the Act.<sup>63</sup> In the said bill, Section 6 and 7 talks about the protection of the personal data and provide the conditions on which personal data can be collected with the prior consent of the person. But the best part is that section 8 of the bill prohibits the storage of the personal data for the said granted period. The researcher is arguing for the same thing the collection of data is much easier but storing it and then providing the security to that the toughest thing to deal with. Again, section 11 talks about the security and duty of confidentiality which imposes a duty on data collector that they can only collect the personal data when they have enough resources to save and protect data and violation of which will make them guilty. Section 16 of the said act prohibits everyone from

<sup>62</sup> Editorial, 'WhatsApp privacy policy case: Here's what it says, and why it matter', *The Indian Express*, (29 April 2017) available at <http://indianexpress.com/article/technology/tech-news-technology/whatsapp-facebook-privacy-case-supreme-court-everything-you-need-to-know-4631853/>, accessed on 30 March 2017.

<sup>63</sup> Pankaj Kumar, 'Data Protection Law in India', 2014, *Legal Service India Official Website* available at <http://www.legalserviceindia.com/article/l37-Data-Protection-Law-in-India.html>, accessed on 30 March 2017.

storing sensitive data. Even chapter IV of the Act talks about the constitution of the data protection authority. The researchers have not dealt with the bill in totality as this research is focused on this bill but its ambit is more than that. The main motive behind discussing the Personal Data (Protection) Bill, 2013 is that our privacy jurisprudence is different as our diversity is different from the first world countries. Then we must come with a new solution and according to the researcher, the best solution is to come up with the new law which must be rigid in nature. Things should be made so completed that before dealing with personal data these Tech giants must think twice or thrice. When it comes to the legal point of view the pending bill must be passed and incorporated as soon as it is possible. In August last year, the Government of India had said in the Supreme Court of India that “violation of privacy doesn’t mean anything because privacy is not a guaranteed right”, actually arguing that the citizens of India do not have a fundamental right to privacy.<sup>64</sup> Now, these types of statement given by the Government of India forced us to think that at one hand they are advertising for the digitalization of India and on the other hand they are saying that of personal data security is not their concern. If we are talking about development then for that we have to develop in all the areas then only that development would resist other we will fall as Greece did. It is the time to think beyond the political issues then only we will be able to fight those developed countries. We do not have an authorized copy of that bill; it is leaked by media sources. If our ministries are not able to protect their document, then is it reliable to think that they will be able to secure our personal data? Absolutely not, that is my answer. But this new legislation which is on the web is the dire need of the day. We have witnessed the way Hon’ble Supreme Court dealt with the matter related to Aadhaar. By the time the Supreme Court decides on the issue of Privacy, and the petitions will be rendered infructuous. Hence, the researcher is having an opinion that India does not only need a good judgment but most important is judgment must be on time. Our data is not secured and we do not need any debate on that, it should rather be about having a law and an authority which will secure our data. Since everything in this world is going to be on cyberspace so we need to secure that space so that we can stay a peaceful life.

---

<sup>64</sup> Vivke Pie, ‘Indian Government says it is still drafting privacy law but doesn’t give timelines’, 2016, Medianama Official Website available at <http://www.medianama.com/2016/05/223-government-privacy-draft-policy/>, accessed on 30 March 2017.