LAWFOYER INTERNATIONAL JOURNAL OF DOCTRINAL LEGAL RESEARCH

(ISSN: 2583-7753)

Volume 1 | Issue 2

2023

A STROLL THROUGH THE STATE OF DIGITAL PRIVACY IN INDIA

Kritik. Kumar Jain[1] & Tushar Ahuja[2]

I. ABSTRACT

Since the onset of the internet age, an infamous Data Entrepreneur, **Clive Humby**, proclaimed that **"data is new oil"[3]** and today we are witnessing his assertions turning into a reality as individuals are moving across every direction seeking strategies for ***mining data***, much like oil. certain are morally sound, such as collecting with consent, which is neither coerced nor without our own free will, whilst others frequently accumulate these data unilaterally by forcing us into accepting certain "*terms and conditions*" while without them, we cannot utilize the service given by them.

In addition, there are some cyber-attacks by perpetrators, with the most unsettling usage we have ever witnessed, it's also employed by the governments of several states, including ours, using ***spywares*** to target their rivals as well as other individuals in order to obtain an edge over their rivals.

In this study, we will explore each of these issues in brief, from computer usage to the government exploiting this data for various objectives from ***"segmenting to blocking"***, as well as certain sections of the **Information Technology Act[4]** (hereinafter IT Act) dealing with these attacks on our privacy.

II. KEYWORDS:

Data, Privacy, Government and IT Act.

---

[1] 4th YEAR STUDENT OF BBA.LLB(Hons.) At LAW COLLEGE DEHRADUN, UTTARANCHAL UNIVERSITY.
[2] 4th YEAR STUDENT OF BBA.LLB(Hons.) at LAW COLLEGE DEHRADUN, UTTARANCHAL UNIVERSITY.
[3]Rohit Sharma, 'Is Data Really the New Oil in 2023?' *(upGrad,* Last updated 28Mar 2023),<https://www.upgrad.com/blog/why-data-is-the-new-oil/> accessed on 23rd July 2023.
[4] THE INFORMATION TECHNOLOGY ACT, 2000 (No. 21 OF 2000).

III. INTRODUCTION

Since the beginning of our existence, we as species have invented a plethora of general public technologies that have aided us in revolutionizing the way we live, be it the ***"wheel"*** in our earliest days, or ***"steam locomotives"*** in the eighteenth century, or the ***"Internet"*** today, we have continually acquired an enormous number of gains or have surpassed every constraint to bring about certain significant shifts in the global trends.

However just like any other place in the world the concept of ***"yin and yang"*** also applies herein as just like the positive aspects(benefits) which anything inhibits, we must also face its dark side I.e., repercussions too.

Likewise can be stated about the internet, which enabled us operate on and foster a digital plane upon which we could work, play, meet our friends, learn new things, and an array of other things, but there is also a dark side to all of it where we could see people involved in a variety of malpractices, some with knowledge of their actions and others without any intent or knowledge of the tasks they ought to undertake therein.

Herein we would be discussing many of these ***cybercrime(s)*** and unlawful activities performed by **"people"** of various genre(s) be it the big corporate houses, or the perpetrators, or the government(s), like the ***sovereign*** of our great nation which has used these technologies for their own personal gains.

In addition, we would discuss the efforts done by our legislative bodies and judicial authorities to safeguard our security on the internet.

IV. BREACHES *via* CORPORATE HOUSES

Today we are tied from top to bottom with various devices either; wired or wireless, these devices contribute to our day-to-day workings be it studies, business, research or any other task. Yet all of this is mostly free, and we hardly pay enough for any of it and even

then, they(businesses) are making billions of dollars from all this free stuff while, we enjoy their free services day in and out.

As the saying goes, ***"When you are not paying for the product, You are the product"***[5] the same phenomenon is happening here as: our data, the choices we make over the internet, I.e. our tastes and preferences are being observed and recorded in the form of ***patterns*** over the web and this process is known as **Data Analysis**, one of the most growing fields of today's time as it helps the big-tech oriented enterprises comb through the data and to find out all the necessary information(s) required to gain or make a fortune out of it.

One of the most prominent instances being the **"Google ads"**, which are commercials that have been *diligently customized* by Google for us, so that Google can make money by reposting these advertisements, every time we surf on it for something or the other. While the corporation could prosper via individuals consuming what they sell instead of obtaining those from elsewhere in the world. As the consumer is cognizant that the good or service that he seeks is readily available on the website he visits, the advertising of all of this can often be rendered feasible by the process of analyzing ***big data*** or ***metadata***, subject to the magnitude of the **data sets** provided to the business[6]**.**

V. BIG-DATA ANALYSIS

Even though this process is highly beneficial for the enterprises, we get the shorter end of the stick as it's our *personal data* that they are combing through, yet we don't have any means to stop them or take any *stern action* because of the lacuna of Indian law regime which we will discuss in later stage. Moreover, this process of analyzing the data is called **Big-Data Analysis** wherein businesses collect data from their customers and sometimes

[5] Scott Goodson, 'If You're Not Paying For It, You Become The Product' (*Forbes,* 5th March 2012) <https://www.forbes.com/sites/marketshare/2012/03/05/if-youre-not-paying-for-it-you-become-the-product/?sh=8b2868b5d6ee> accessed on 23rd July 2023.

[6] Megan Graham, Jennifer Elias, 'How Google's $150 billion advertising business works' (*CNBC,* 18th May 2021) <https://www.cnbc.com/2021/05/18/how-does-google-make-money-advertising-business-breakdown-.html> accessed on 25th July 2023.

potential customers or prospects. This data comprises of; name, mobile-number, e-mail id and sometimes recent history I.e., all the things we shop, what we add to our cart(s), or the kinds of payments methods used or pins, card details etc. which they put through ***sophisticated data analysis processes*** to gain valuable insights from the pool of data collected therein.

VI. ISSUES AND RELATED CASE-STUDIES

But there are a lot of problems in it some due to **lack of due diligence** by the companies and other through **outside interventions** which leads us to the next point of discussion, the **Hack(s)** onto the servers of these companies which induces potent threat on our **digital privacy** as these instances narrates a lot of data of our personal importance being sold on the dark web for free or for bitcoins and these occur more frequently than ever, as within the first half of the current year we've witnessed about two major incidents:

Firstly, the attack on the servers of **AIIMS**[7] & **Secondly,** it was reported that another attack had taken place on **HDFC Bank**[8] recently where the data of over *six-lakh customers* is being released in the dark web containing sensitive customer data such as name, date of birth, phone number, email address, physical address, employment information, credit scores, loan information, and moreover the bank has denied these claims whereas, in the AIIMS attack the authorities have claimed that no information was leaked but, if it had happened it would have been a catastrophe due to the presence of critical information I.e., the **Sensitive personal data(s)** of millions of people if not billions, was contained in these servers.

[7] ET Online, 'Cyber-attack on AIIMS Delhi's servers originated in China, say government sources' (*The Economic Times*, 14th December,2022) <https://economictimes.indiatimes.com/news/india/cyber-attack-on-aiims-delhis-servers-originated-in-china-says-mohfw/articleshow/96222031.cms?from=mdr> accessed on 22nd July 2023.
[8] Singh Rahul Sunilkumar, 'HDFC Bank users confidential data leaked, claims hacker; bank denies' (*Hindustan Times*, 9th March 2023) <https://www.hindustantimes.com/business/hdfc-bank-users-confidential-data-leaked-claims-hacker-bank-denies-101678361981623.html> accessed on 25th July 2023.

Another elephant in the room is the **"Aadhar Data Breach,"**[9] which affected practically the whole nation. As we witnessed the world's largest database being compromised, seeking personal information(s) such as; 12-digit Aadhar number, Biometrics, Retina scans, Addresses, Pictures, and the unique details of literally every member of the population of India, as the breach allegedly touched about **1.1 billion individuals**.

In this cyber-realm these attacks are happening again and again one after the other, inducing potent threats not only on **Organizations** (businesses, banks, hospitals), or **Individuals** (prudent civilians) but also on the **Sovereign** of the states all around the globe.

VII. KINDS OF ATTACKS

The breaches not only occur on groups but also on individuals wherein attacks like **Phishing** or tracking an individual are of common occurrence but, we've seen some new kinds of attacks like: Spear-Phishing, voice cloning and other new trends which are being utilized by the attackers to gain something or to stir up some tensions in the society. The best example of it is **Voice-cloning** where the hackers use the voices of the top executives of a company to give command to employees to transfer some funds from the accounts of the company to their respective accounts and the employee does it without cross-verifying due to the call(s) being from the higher authorities while, In **Spear Phishing or Whaling** the hackers use the concept of big data analysis to find potential targets to cheat upon or simply try to find the clients with deep-pockets and target them.

As the AI powered age evolves, it is now viable to easily create a cloned voice by gathering specimens from one of the target's social media handles, reels, or videos, or through voice messages, which they then put onto either free or paid software(s) to clone within a matter of minutes subsequently, all they've got to do is track down a target

[9] Abi Tyas Tunggal, 'The 70 Biggest Data Breaches of All Time [Updated April 2023]' (*UpGuard,* 18th July 2023) <https://www.upguard.com/blog/biggest-data-breaches> accessed on 25th July 2023.

susceptible to **spear phishing** and come up with a tempting story. The finest illustration of this could potentially be found in **Apple's IOS.17**, which enables users to achieve this by uploading certain E-samples to their iPhones, which cultivates an incredibly identical tone to that of the owners' overnight[10].

VIII. ETHICAL SPAMMING: PERMISSABLE OR NOT?

However, there is an ethical way of spamming here too, wherein the companies use the data of their consumers and sell it to other companies as their potential clients and this practice is done by almost everyone in the industry. For e.g. When we login to an application for purpose of trading shares after sometime we will start previewing ads and messages related to the Stock market and various other related things as if, someone is shouting on the digital world that, so and so has started trading using so and so application and we can't do anything about it as it's the price that we pay for accessing these services for free, as nothing is free in this world.

IX. OFFENSES PUNISHABLE U/R IT ACT 2000

Next point that we would touch upon is the serious crimes that are in violation of our privacy and the ones that the government had taken some actions to curb out though we could still see them occurring a lot, offenses like **cyber stalking**, **sharing of private photos of individuals**, **misrepresentation, fabrication of e-documents** and others like the **tampering with computer resources** of people which affects the privacy of individuals in cyber world have been penalized by the government of India under the **IT ACT 2000**, yet there is a lot of work left to be done in this area.

For example, with the biggest avenues being the **"Personal Data Protection Laws" t**o safeguard one's *personal data* and *sensitive personal data privacy* and to hold someone

[10] Amy Bunn, 'Artificial Imposters- Cybercriminals Turn to AI Voice Cloning for a New Breed of Scam' (*McAfee,* 15th May 2023) <https://www.mcafee.com/blogs/privacy-identity-protection/artificial-imposters-cybercriminals-turn-to-ai-voice-cloning-for-a-new-breed-of-scam/> accessed on 25th July 2023.

accountable in the case of a breach. Although the IT Act also works in this domain, but its work(s) are limited. As the IPC is in the cyber realm wherein, we could use it **partially** to penalize the said perpetrators during trials but not **"fully".** Yet, our own legislature is unable to pass personal data privacy law(s) ever since the report of **Justice Srikrishna Committee** of 2018, set up by **MeitY**[11] which in its reports clearly stated that the ***"personal data protection laws are the need of the hour"***[12]**.**

X. PEGASUS & THE ROLE OF INDIAN JUDICIARY

Although in some cases our guardian has also tried to hack into our privacy through the weapon named **Pegasus** a spyware which our government had allegedly used on its citizens to spy on their opponents and others to which our Apex court put an end in the case of **Manoharlal Sharma vs Union of India**[13]**.** These offenses when paired with all the frauds and identity thefts and other kinds of cyber- crimes constitute the bulk of crimes that take place not only in our country but across the globe and all pose some or other kind of danger to our digital privacy which we often consider to be protected by law. While a lot of work has been done by our law makers in this direction, where our judiciary took the biggest step in this direction when they declared *Right to Privacy* as a Fundamental right which included **8 kinds of privacy**[14] under this right in which one of the kind was the ***"right to informational privacy"*** a right which understands that the digital privacy over the internet is a myth and tends to protect it and in the ***"Pegasus judgement"*** [15] wherein the judiciary even commanded that government cannot violate our privacy under the pretext of national interest. While the legislature did it part by creating the IT Act 2000 whose various provisions dictate penalties for those who violate

[11] Ministry of Electronics and Information Technology.
[12] Suprita Anupam,'The DPDP Bill Does Little To Protect The Fundamental Right To Privacy: Justice BN Srikrishna' (*Inc 42,* 24th November 2022) <https://inc42.com/buzz/the-dpdp-bill-does-little-to-protect-the-fundamental-right-to-privacy-justice-bn srikrishna/#:~:text=In%20July%202017%2C%20the%20ministry,submitted%20its%20draft%20in%202018> accessed on 25th July 2023.
[13] Civil/Criminal Jurisdiction, Writ Petition No. 314 OF 2021.
[14] *Justice K.S. Puttaswamy and Anr. Vs. Union of India (*2017) 10 SCC 1, AIR 2017 SC 4161.
[15] Manoharlal Sharma vs. UOI (n 11).

our privacy, our digital plane under various sections of the Act like, the compensation for failure to protect our personal data under **section-43A** and various other punishments for those who fail to protect our privacy in the digital plane under **section-66** and its various counterparts which talks about attack on informational privacy over the internet and **section-67** and its various parts which talks about prevention of bodily privacy. In addition to this, Parliament has also added a provision for the *National Nodal Agency* in **section- 70(A)**, creation of ***CERT-IN* 70(B)** which played an important role in the above-mentioned AIIMS attack.

Moreover, they've also talked about declaring a *"Protected System"* under **section- 70** and about construction of an **Appellate Tribunal** for laws pertaining to cyber space in **Chapter-X** of the IT Act 2000. In addition to all this it also persists legislations for Extra-territorial activities under the ambit of **section- 75 r/w section-1(2)** while it's **section 81** provides an overriding effect which makes it the most prominent player in the field of cyber jurisprudence.

Though the IT Act is robust and may seem indestructible at a casual glance, it has its shortcomings too as; most of its punishments are bailable offenses to which an offender could easily be granted bail and can tamper with the evidence.

The next point of concern is that the offenders are not easy to catch so a concept like ***Strict liability*** can help a lot and the act also has a lot of other concerns like the extra territorial activity of the act is just for the namesake as our nation has not signed any extradition treaty concerning it and the biggest problem of all is the absence of a ***Personal Data Protection Act*** to protect our privacy from the big corporations who are selling it in bundles or due to whose negligence our privacy is being sold on the dark web. Unlike the European Union and USA our **Personal Data Privacy Bill** has been on the table of Parliament for the last four years.

XI. CONCLUSION

In the tail end of this article, we assert that, regardless of residing in the nation with the **second highest number of internet users**, our *Right to Privacy* on the **digital plane** has yet to be fully protected by our government, and that, with the number of cyber-attacks increasing by the day, Is our government just too naive in understanding how susceptible its national(s) are in the digital realm ? Or are we just awaiting a larger catastrophe to strike, like in the case of the **26/11 attacks**, which spurred us to consider modifying the IT Act to be compliant with domains dealing to cyber terrorism, among other things, or are we waiting for another gigantic catastrophe? While our government is acting in a lackluster manner in dealing with issues threatening our privacy. We urge our readers to carry themselves appropriately on the Internet by not falling for **"things that are too good to be true"** or **"operating naively"** by uncovering data that could potentially be utilized against them or prove to be a disgrace to them in the later half.

In the conclusive remarks, we need to emphasize the need to be **"a human firewall"**[16] over the internet and that how crucial it is to play intelligently and break the chain of these events, whether it is not falling for fake phishing scams or sharing information over the Internet to protect large incidents such as the **Assamese-Exodus** and a variety of large and small cyber-attacks.

[16]'Your Human Firewall – The Answer to the Cyber Security Problem | Rob May | TEDxWoking' (*TEDx Talks,* 29th November 2017)<https://youtu.be/BpdcVfq2dB8> accessed on 25th July 2023.