VOLUME 16 ISSN 2456-9704

THE ERA OF BIG DATA: PRIVACY IN QUESTION

By *Saumya Tripathi and G. Brahmakrit Rao From Symbiosis Law School, Hyderabad and Symbiosis International University, Pune; respectively*

ABSTRACT

Privacy is a Fundamental right recognized by many International organisations like UN, ICCPR, etc. The researcher in this paper aims at determining the perks of Big Data, but moreover tries to culminate how privacy and data protection is being hindered or challenged by this. Initially the paper seeks to make the reader understand and incorporate as to what is meant by Big Data in the contemporary scenario. Later, data protection issues and privacy issues have been made to come in picture, along with how government keeps a balance between surveillance and right to privacy as enshrined in the Indian Constitution. CCTV footage and recordings as such kept at the behest of the state is also being questioned as to whether this violates the right to privacy of the general public or does national security plays a trump card over such Fundamental Rights. To conclude, the paper will try to explore policies, laws and regulations made by the government to protect user data in such digital era, and the researcher will also give their own recommendations as to how the present state of affairs could be improved.

Keywords: United Nations, ICCPR, Right to Privacy, big data, CCTV.

INTRODUCTION

Right to Secrecy is considered a right naturally perceived by the UN. It's hard ere characterize compactly what's more, unequivocally what this right entails. Protection has a double perspective- it is worried about data or on the other hand close to home information & the degree to which that is common with different gatherings. The comprehension of security[1] has been formed by advancements accessible at the time, beginning from proficiency, to accounting to papers, & the present occasions we live in, the Internet. The Internet & the approach of mass information gathering & maintenance have reshaped the idea of protection in the advanced world. The current talk around protection rotates around the ways in which outsiders manage the data they hold-regardless of whether it is verified, defended, who approaches, & under what conditions. The 'right to protection' is an essential natural right perceived in the universal declaration of natural vagrant workers also, the UN convention on protection of child in numerous other universal & local arrangements. Various worldwide natural rights contracts, shows & natural rights courts give explicit remark to protection as a right.

The UN special speaker made remark to one side to protection in his first report on eighth march 2016. Two standards support his report: **(A)** Security protections must be accessible paying little mind to national fringes; **(B)** Solutions for infringement[2] of protection similarly should be accessible over these matters. So, as to encourage the Principles, the special Speaker[3] has additionally plot a ten point action plan.

The privilege[4] to protection supports different rights & opportunities like the opportunity of articulation, affiliation & conviction. Notwithstanding, in the period of huge information, the privilege to security has turned into an urgent issue close to home information is routinely

gathered & exchanged the new economy. Information specialists furthermore, investigators are presently attempting to recover protection concerns & guarantee that data is secured.

In the present age 'interchanges reconnaissance'[5] envelops the "observing, capturing, gathering, getting, breaking down, utilizing, protecting, holding, meddling with, getting to or comparable moves made with respect to data that incorporates, reflects, emerges from or is about an individual's correspondences previously, present or future." (Necessary & Proportionate Alliances, 2014)

The "Big" is huge information which alludes to volume, yet in addition the speed & assortment of information components & sources. These huge databases are gathered by government to give welfare benefits yet overseen or put away by private partners or gathered by private innovation Companies. For instance, in India, Unique Identification Authority of India (UIDAI), Census of India, Stock Exchan . The Ministry of Rural Development for the Mahatma Gandhi National Rural Employment guarantee annual tax department among others hold enormous datasets. Aside from these, different projects of I

ndian Government like Central Monitoring System, Natural DNA Profiling,Smart Cities Missions & Digital India Program to hold enormous information. Other than the administration, non-state on screen characters including telecom suppliers, online travel agencies utilize huge information examination to advance their organisation. In spite of the fact that there are certain qualities of enormous information situated projects have an unmistakably laid down protection arrangement, there is an absence of appropriately explained access control component & questions over significant issues, for example information proprietorship owing to most undertakings including open private association which includes private associations gathering, handling, & holding a lot of information.

Hence, the Natural Rights ramification of

---

[1] For example, the 1950 Convention for the Protection of Human Rights and Fundamental Freedoms, the European Convention on Human Rights, the American Convention on Human Rights, and the American Declaration of the Rights and Duties of Man. Several Courts of Human Rights have also begun to address privacy issues in their hearings.

[2] An American computer professional, former Central Intelligence Agency (CIA) employee, and former contractor for the United States government who copied and leaked classified information from the National Security Agency (NSA) in 2013

[3] Ten Point Action Plan will be discussed later in the sub-section 1.1. under 'Privacy Safeguards at the International Level

[4] Report of the United Nations Special Rapporteur on the right to privacy, (A/ HRC/31/64). 8th March 2016, seen at 4th October, 2019, 14:51.

gathering, stockpiling & utilizing enormous information in the Indian setting should be examined. The paper investigates the issue of security in the huge information age & how enormous information assembled through ICT apparatuses & online life stages can be utilized against residents. This paper will likewise break down the significance of security & depict the advances that put natives' information most in danger on the net. At long last, the research will recognize potential approaches to secure residents private information on the internet.

[5] The US, the United Kingdom (UK), Australia, Canada, and New Zealand are the Five Eyes Intelligence Alliance. See: Nyst, C and Crowe, A. Unmasking the Five Eyes' global surveillance practices. Association for Progressive Communications (APc) & Humanist Institute for cooperation with developing countries (Hivos). APC-201408-CIPP-R-EN-DIGITAL-207.

RESEARCH OBJECTIVE

One of the objectives of this research paper is to understand, keeping in mind the Indian perspective, as to what meant by Big Data and does it pose any threat to the citizens if it is not regulated by the government. The research paper also tends to explore whether CCTV cameras which come under the surveillance by the government hinder right to privacy of the general public or an individual person per se. the paper also strives to target as to how human rights of a citizen gets violated when such data is being misused by tech companies and the government.

RESEARCH QUESTIONS

1. What are the diverse protection issues identified with utilization of Big Data?
2. In what capacity can enormous information assembled through ICT devices & stages, including online networking be utilized against clients?
3. Can CCTV Footage be considered as issue of privacy in the era of Big Data?
4. What can be possible solutions for the above mentioned issues?

Chapter- 1

BIG DATA & ITS RELATIONSHIP WITH PRIVACY

The nation is encountering revolution of data[6]. Now-a-days, an immense proportion of data is ordinarily being made and spilling out of various sources, through different channels, reliably in the present computerized age. Research has demonstrated that measure of data put away every year developed to 161 exabytes, up from 5 exabytes in 2003. Generally, equivalent to the measure of data put away in the size thirty seven thousands of library as that of "US Library of Congress."

Big Data is another worldwide of information driven choices. The amount of information that is being created by cell phones, TV's, web based life styles, sensor driven gadgets & numerous other such arranges that we always use in our everyday life. Big Data searches for connection as opposed to the causation, the 'what' as opposed to the 'why'. Big Data contains an assortment of information types including content, symbolism & video. Various wellsprings of such information[7] types are standard news stories, internet based life

stages, pictures on Instagram, proficient photos, satellite symbolism & elevated symbolism caught by unmanned Aerial vehicles (UAVs), & recordings from TV channels , "YouTube", & various channels. This isn't constrained to the created world, with the creating world delivering enormous measures of huge information also rapid ICT improvements & client's commitment with stages like social media, miniaturized scale blogging destinations, among others empower extraordinary social occasion, maintenance, & examination of enormous data. The information gathered from web based life, sites, portable GPS, & more could help to address different viable arrangements & measures. Hence, enormous information is being considered as an uncommon asset that could possibly present interesting chances for all. Alongside big data, metadata, likewise can possibly uncover delicate data about individual's lives, political inclinations, religion, sexual direction, & so forth. The plan of action of numerous web organisations depend on the gathering of metadata, so as to improve their administrations & to deduce clients conduct to further improve their items. Be that as it may be, gathering, getting to & utilizing such information convey huge dangers to key opportunities & natural rights. Big data & metadata[8]

both have the potential to truly undermine people's privileges to keep their own what's more, touchy data privilege & to have power over how their data is utilized.

As of late, political pioneers & organisations are declaring big data as an answer for differing scope of issues from defilement, giving taxpayer supported organisations, battling against maladies & so forth. It has been noted that for the sake of open administrations, better conveyance of resident driven administrations, better client experience & giving security also, security of natives, governments & private partners are collecting, putting away & breaking down gigantic measures of resident's information. Be that as it may, worries over the absence of straightforwardness & responsibility[9] around the plan of calculations process used the information, questionable measures of security utilized away & upkeep of huge databases & overreliance of enormous information rather that customary types of investigation & the formation of new advanced partitions have developed. In the next segment, I will talk about how governments & various organisations are gathering, putting away, utilizing, moving & reusing gathered information for various objectives & how the privilege to protection is being compromised & encroached upon in the immediate time of big data.

At long last, in view of the "Ten Point Action Plan" proposed by UN exceptional speaker

---

[6] Data that gives a description of data

[7] "Personal data" means data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller'.(Sept 27, 2019, 3:31 pm) See: https:// www.dataprotection.ie/docs/What-is-Personal-Data-/210.htm

[8] Metadata summarizes basic information about data, which can make finding and working with particular instances of data easier

for the privilege to security, the paper propounds to create a system in India to secure native's close to home & touchy information on the internet. Toward the end, the paper diagrams a few open doors for gaining ground.

PRIVACY PROTECTION AT AN INTERNATIONAL LEVEL

A few nations have protection shields for their very own residents. Protection is a major natural[10] right perceived in the "Universal Declaration of Natural Rights (UDHR), the International Covenant of Civil & Political rights (ICCPR), the UN Convention on Migrant workers & UN Convention on Protection of Child's & in a few other universal & territorial settlements, various global natural rights contracts, shows & natural right courts give explicit remark to security as a privilege.

[9] 'Sensitive data encompasses a wide range of information and can include: your ethnic or racial origin; political opinion; religious or other similar beliefs; memberships; physical or mental health details; personal life; or criminal or civil offences. These examples of information are protected by your civil rights.' (15th Sept, 2019, 12:23) See: http://web.mit.edu/infoprotect/docs/protecting data.pdf

[10] For example, The 1950 Convention for the Protection of Human Rights and Fundamental Freedoms, the Convention created the European Commission of Human Rights, the American Convention on Human Rights, the American Declaration of the Rights and Duties of Man. Also different Courts of Human Rights have also begun to addresses privacy issues in its cases

Article 12[11] of UDHR provides that

"*No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour & reputation. Everyone has the right to the protection of the law against such interference or attacks."*

The ICCPR in Article 17 provide that

"*No one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour or reputation."*

It additionally says "everybody has the privilege to the security of the law against such observations or attacks." The United Nations General Assembly (UNGA) in its goals, worldwide natural rights law gives the all-inclusive structure against which any obstruction in person security rights must be surveyed. Other territorial bodies, for example, the EU, perceive the privilege to security as a basic natural right in "Article 8 of the Charter of Fundamental Rights of the European Union." The special Speaker on the advancement & security of the privilege to opportunity of feeling & articulation can't be completely enjoyed. During the thirteenth meeting in December 2009[12], in UN the discussion on the advancement[13]. Furthermore, assurance of natural rights & crucial opportunities, Frank La Mourn, likewise underlined that, "reconnaissance frameworks require compelling oversight to limit hurt & abuses." Including by requiring a warrant issued by a judge on a case-by-case premise. The Ten point Action Plan[14]

outlined is:

1. Going past the current lawful structure to a more profound comprehension of what it is that we have promised to secure.
2. Expanding mindfulness.
3. The protection of an organised, on-going discourse about protection.
4. A complete way to deal with lawful, procedural & operational defends & cures.
5. A recharge accentuation on a specialised protections.
6. An uncommonly engaged exchange with the corporate world.

[11] See the Article 12 of the Universal Declaration of Human Rights (UDHR), 1948.

[12] See A/HRC/27/37 also available at http://www.ohchr.org/EN/Issues/DigitalAge / Pages/DigitalAgeIndex.aspx

[13] Report of the United Nations Special Rapporteur on the right to privacy, (A/HRC/31/64). 8th September 2019 15:04.

[14] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. (A/HRC/23/40). Human Rights Council. Twenty-third session. Agenda item 3. Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development Frank La Rue

1. Advancing national & territorial advancements in security assurance systems.
2. Bridling the vitality & impact of common society.
3. The internet, cyber-security, cyber-secret activities, cyberwar[15], & cyber peace.
4. Putting further in International law.

PRIVACY ISSUES IN REMARK TO INDIAN CONSTITUTION

The Supreme Court of India has in various decisions saw the suitable to security as a subset of the greater perfect to life and individual opportunity under Article 21 of the Constitution of India. The article communicates that no individual will be prevented from securing his life or individual opportunity beside as shown by procedure developed by law. The Supreme Court of India has expressed that Article 21 of the Constitution is the middle for major rights. The extension in the components of Article 21 has been made possible by giving a comprehensive significance to the words 'life' and 'opportunity'.

The extend of the right previously came up for thought in "*Kharak Singh v. Sttae of Uttar Pradesh*"[16], which was worried about the legitimacy of guidelines[17] that allowed the reconnaissance of doubts. In the setting of article 19(1) (d), the privilege to security was again considered by Supreme Court in 1975, while choosing the instance of *Govind v. State of Madhya Pradesh*[18], it sets out different essential benefits of inhabitants can be delineated as adding to the other side to assurance. Regardless, the Supreme Court furthermore communicated that the benefit to insurance would need to encounter a method of case-by-case improvement.

The SC in the instance of *R. Rajgopal v. State of Tamil Nadu*[19], just because straightforwardly connected the privilege to protection to Article 21 of the constitution is verifiable justified to life & freedom ensured to the residents of this nation by Article 21.

It is a 'right to be not to mention.' A native has a privilege to defend the security of his own, his family, marriage, child, parenthood, tyke bearing & instruction among different issues. No one can distribute anything concerning the above issues without his assent whether honest or generally & whether commendatory or basic. In the event that he does as such, he would abuse the privilege to

[15] See The right to privacy in the digital age. Report of the Office of the United Nations High Commissioner for Human Rights (A/HRC/27/37)

[16] Kharak Singh v State of UP, AIR 1963 SC 1295; People's Union of Civil Liberties v. the Union of India, (1997) 1 SCC 318

[17] Kharak Singh v. State of Uttar Pradesh, cited at: (1964) SCR (1) 332.

[18] Govind v. StateofMadhyaPradesh, cited at: AIR 1975 SC 1378.

[19] R. Rajagopal v. State of Tamil Nadu, cited at: 1994 SCC (6) 632

protection of the individual concerned- on account of *PUCL V. Association of India*[20], the Supreme Court saw that phone tapping would be a genuine attack of a person's privacy.

In remark to "*Selvi v. State of Karnataka,*[21]" the SC said that an automatic subjection of an individual to narco investigation, polygraph assessment, BEAP tests damages the privilege to privacy. It is noticed that with the expanded extent of Article 21 of the Constitution covering appropriate to protection, yet any person's security is registered because of the absence of legitimate strategy & structure.

The thoughts of protection & information the board that are passive can be followed to the "Fair Information Practice Principles (FIPP)." These standards are additionally followed in worldwide systems, for example, the "OCED privacy guidelines, APEC" structure or the nine national privacy principles enunciated by the Justice A.P Shah Committee Report. In 2002, the Justice A.P Shah board suggested a overall legislation to secure protection & individual information in private & open circles. The report likewise proposed setting up protection chief's both at central & state levels. Nine national security rules that can be perused while surrounding the law. The Supreme Court saw that the benefit to security[22] may be restricted for evasion of bad behavior, issue or security of prosperity or morals or confirmations of rights and chances of others. Tragically, during the thinking about a lot of petitions hoping to stop the utilization of the Aadhar Scheme in July 2015[23], the inside replied in the Supreme court that insurance was not a pivotal right in India. Legal advisor General Mukul Rohatgi said the benefit to insurance had been a 'vague' thought, all of these occasions, a subject of changing closures from SC. These systems give the intensity of consent fore people with the goal that they ought to be informed if their own information is utilized.

PRIVACY IN RESPECT OF ACCESS BY STATE

Another part of enormous information is the deceptive access of individual information by the state[24]. Numerous nations are gathering & refreshing their resident databases for example Huge

[20] PUCL v. Union of India, cited at: (1997) 1 SCC 30.

[21] Selvi v. State of Karnataka, cited at: AIR 2010 SC 1974.

[22] Social Credit comprises interlocking concepts of economics and politics which deal with the just relationship between man and the Society in which he lives.

[23] See Report of the Group of Experts on Privacy (Chaired by Justice A P Shah, Former Chief Justice, Delhi High Court) 17th September, 2019, 1:12 am, http://planningcommission.nic.in/reports/genrep/rep_privacy. pdf

[24] The survey was conducted by the Pew Research Center. It is a nonpartisan American think tank which is based in Washington, D.C. It provides information on social issues, public opinion, and demographic trends shaping the United States and the world.) 17th September, 2019, 1:12 am, See: http://www.pewresearch.org/topics/privacy-and-safety

Data Bank to incorporate biometric identifiers that confirm character dependent on physical attributes for example physical attributes, for example, fingerprints, iris, face & palm prints, religion, ethnicity, sexual direction, walk, voice & DNA. Mandatory national distinguishing proof frameworks[25] have been executed in various nations counting "Argentina, Belgium, Colombia, Germany, India, Italy, Mexico, Peru, Spain & Thailand (Electronic Frontier Foundation)."

For instance, Aadhar task of India gathers all inhabitants' biometric data. It has turned into a device for focused reconnaissance & mass observation to clandestinely distinguish what's more, track residents. Aadhar has turned into the accepted personality archive acknowledged at private banks, schools, emergency clinics, telecom administrations to purchase SIM cards, medical protection or some other utility administrations. The record is being connected to various social plans too. In addition, Aadhar there are other such purported activities, for example, Central Monitoring System (CMS), keen cities mission, & Digital India program that are utilizing innovations furthermore, arrangements[26] that undermine singular protection. Along these lines if individuals or gatherings, the state is likely previously following their developments through web based life, protection organisations, cell phones & so forth.

The Pakistani Government is occupied with interchanges observation-of telephone what's more, web connection 9IP) traffic, locally, globally & other information like biometrics & gadget enlistment data to counter 'inward what's more, outer' dangers. Biometric server farm has been set up by China with an expressed motivation behind keeping up open security, however has permitted an on the web business venture offering biometric information coordinating administrations access to the information. As indicated by BBC, by 2010, everybody in "China" will be tried out a tremendous national database that arranges financial & government data, counting minor petty criminal offences. The aims behind executing these national recognizable proof plans fluctuate by nation. In most cases, people are regularly appointed an ID number with biometric subtleties, which is utilized for an expensive scope of recognizable proof purposes. Enormous sums of individual & delicate information of occupants, for example, name, date, & spot of sex, biometric information, current location, photos & other data like relatives is connected

to this ID number & put away in an incorporated

[25] This is to prevent identity fraud and theft: governments in Mexico, India, and Argentina are all developing Biometric national identification systems and Thailand has launched a smart ID card that is believed to be the largest integrated circuit chip ID card project in the world

[26] UNHCR (http://bit.ly/1THlwlH) uses biometric technologies to process enrolment in refugee camps, the World Bank () to ensure effective targeting of beneficiaries, by funding biometric systems for registration of the urban poor in Benin and Kenya. 18th Sept, 2019, 05:10.

database. Government[27] chiefly make big data banks for the scope of purposes, including national recognizable proof frameworks, constituent registers & supporting demoratization[28]- Phillappines (Jaracz, 2013), Ghana (Darkwa, 2013) furthermore, Kenya(Kisiangani & Lewela, 2012) guide conveyance & social assurance programs. While supporters claim that biometric identifiers an compelling approach to precisely perceive individuals, they are costly & inclined to mistake & above all, abuse to their own information. Furthermore, the developing concern is that huge information advances can possibly be used to oppress helpless gatherings & control data. Biometric identifiers present outrageous dangers to person's security & can make a disturbing impact on appropriate to protection, opportunity of articulation & opportunity of getting together & affiliation on the web & disconnected.

[27] Mauritania is implementing a biometric entry-exit border control system as part of its security and counter- terrorism strategy and Senegal (http://www.snedai.sn/fr/) recently implemented a biometric visa process upon entry for nationals of certain countries

[28] The real-time statistics gathered at 13:12 (Indian Standard Time) on 15/08/2019. Source: https://uidai.gov.in

Chapter 2

PRIVACY AND CCTV FOOTAGE

"There was obviously, no chance to get of knowing whether you were being viewed at any given minute… you needed to live, did live, from propensity[29] that wound up impulse, in the suspicion that each solid you made was caught, and, aside from in haziness, each development investigated"[30]

Government observation camera projects[31] represent a few grave worries for common freedoms. To begin with, the presence of the cameras themselves conveys noteworthy security suggestions. The possibility of 24-hour observing of open spaces with video reconnaissance cameras makes a huge amount of data on residents accessible to the government, permitting the observing or following of individuals taking part in completely honest what's more, unavoidably ensured conduct.

The risk to protection is intensified by the innovative advancement of new frameworks. The cameras being introduced and considered by urban areas in California are not the grainy observation cameras of days of old. Many are cutting edge, roosted high on utility poles with 360-degree sees, moving 24-hours per day[32]. With their DVD-

quality video and alternatives for sound, they can zoom in close enough to peruse and record the book somebody is conveying, the name of the specialist's office somebody is entering, or the substance of the individual somebody is conversing with or kissing farewell. Everything the camera sees, or conceivably hears, can be put away on its hard drive or a focal factor in perpetuity.

The ramifications of free to video observation film is wide and has not by and large been considered by arrangement creators. Contingent upon what number of cameras[33] are sent and where they are found, individuals from the open would have the option to ask for and get to video pictures for an entire host of intrusive reasons (for example an untrusting spouse or wife

[29] Feldman, D. 'Secrecy, Dignity or Autonomy? Views of Privacy as a Civil Liberty' (1994) 47 (2) Current Legal Problems .41' Feldman, D. 'Privacy related rights and their social value' in P Berks (ed), Privacy and Loyalty (Oxford Clarendon Press, 1997) 15.

[30] George Orwell, http://www.iosrjournals.org/iosr-jhss/papers/Vol.%2023%20Issue12/Version - 2/B2312020408.pdf (12th September, 2019, 13:01

[31]https://timesofindia.indiatimes.com/home/sunday-times/deep-focus/CCTV-playsSherlock/articleshow/51960067.cms4th 4th October, 2019, 14:56

[32] https://www.thequint.com/india/2015/04/07/needed-norms-on-cctv-usage-in-public-spots 6 Narayanan, Vivek," How Safe are our CCTV Cameras?", The Hindu, Bengaluru, 8th September 2019, 12:09

[33] Agarwal, Surabhi, "Violation of privacy through CCTV cameras rampant, say experts." Business Standard,New Delhi, October 4,2019, 18:16 http://www.business-standard.com/article/current-affairs/violation- of-privacy-throughcctv-cameras-rampant-say-experts-115040400775_1.html

needing to check whether their mate was entering or leaving a home or business that happened to be in scope of a camera, a contradicting political applicants needing to discover who is going into and out of an adversaries[34] battle central station, a political association needing to recognize individuals from the resistance who happened to have a rally inside eye-shot of the cameras. Widespread video observation frameworks may rapidly annihilate the capacity for people to keep their exercises private, not simply from the government, yet additionally from other private gatherings.

IS PRIVACY IN QUESTION DUE TO THE CCTV CAMERAS BEEN INTALLED AT EVERY PLACE?

Barefaced abuse of close circuit TV (CCTV) cameras introduced in retail shops, lodgings & open spots is a "de facto norm"[35] in India. For the offense, instances of which are increasing regularly, one can take lawful plan of action under section 66E of the Information Technology Act, 2000. Up until now, notwithstanding, there has been no revealed conviction under the arrangement.

Digital law specialists state a few instances of introduced CCTV cameras disregarding security are rising, be it cameras introduced in lodges of representatives, in changing rooms of shopping centers or out in the open

& private washrooms. As of late, a 18-year-old worker of a mainstream parlor & bar in Mumbai was captured after he was found recording ladies in the can, through a cell phone taped to the divider. There are occurrences of such infringement on a standard premise in lodgings of honeymooners, which discover their approach to pornography film on the web.

Absence of itemized enactment & solid punishments, just as low mindfulness among the overall population about the entanglements of being under observation, are a portion of the purposes for the rising number of such occasions[36]. The way that India neither has a nitty gritty information security law nor a protection law just intensifies the worry.

[34] Bagchi, Shrabonti, "Growing CCTV penetration creates culture of Surveillance",The Times of India, Bangalore, October 3, 2019, 15:06 http://timesofindia.indiatimes.com/city/bengaluru/Growing-CCTV- penetration-createsculture-of-surveillance/articleshow/39509942.cms

[35] Agarwal, Surabhi, "Violation of privacy through CCTV cameras rampant, say experts." Business Standard,New Delhi,October 4, 2019, 16:50, http://www.business-standard.com/article/currentaffairs/violation - of-privacy-through-cctv-cameras-rampant-say-experts-115040400775_1.html

[36] Rustagi, Geetika, "Indian law only determines the situations where privacy will be afforded legal protection," Live Mint, September 5, 2019, 4:19 http://www.livemint.com/Consumer/x32Rcm7l26gT1cRNMDPAMP/Indian- lawonly-determines-the-situations-where-privacy-will.html

"Computerized voyeurism is progressively drastically in India on account of the expansion of cell phones with cameras & the simple accessibility of government agent cameras. A fast study of Indian erotic entertainment online will affirm its vast majority is doubly unlawful - in light of the fact that generation of sex entertainment is illicit & on the grounds that it has been created because of advanced voyeurism," says Sunil Abraham, official chief of the Centre for Internet & Society, a Bengaluru-based research organization[37]. Gigantic utilization & courses of these clasps bring about the privileges of ladies being encroached over & over, he includes. "It is a horrendous circumstance."

The IT Act, 2000, is the parent enactment to manage electronic reconnaissance. In the event that a camera catches pictures of the private pieces of an individual, male or female, or transmits such pictures without assent, the wrongdoer can be reserved under area 66E.

In any case, the arrangement is a "toothless marvel", as it is a bailable offense, with just three years of detainment & a fine of Rs 2 lakh, says digital law master & Supreme Court advocate Pavan Duggal. He includes since there are no unmistakable rules on the best way to catch (the organization), save (the term) & present the CCTV camera film, examinations concerning such violations aren't done appropriately, prompting no feelings up until this point.

"Our law is evidently needing on the grounds that this isn't the first run through this has occurred; cases are being accounted for from time to time. The absence of measured harms encourages the guilty party," says Duggal.

Under the IT Act, if a camera catches revolting electronic data, the proprietor of a CCTV camera can be reserved under section 67, however on the off chance that the camera catches explicitly express data, it is delegated a non-bailable offense under area 67a, involving five years of detainment & a fine of Rs 10 lakh.

There are occurrences of CCTV cameras[38] being introduced in schools, which is a greater issue, as it may commensurate to youngster sex entertainment.

[37] See the description in the research study conducted by Martin Gill & Angela Spriggs, employees of the Home Office Research, Development and Statistics Directorate, published February 2005, "Assessing the impact of CCTV",p.12,accessible 3rd October, 2019, 15:09 at:http://webarchive.nationalarchives.gov.uk /20110218135832/http://rds.homeoffice.gov .uk/rds/pdfs05/hors292. pdf"

[38] To give an exemplary impression of today's possibilities, the panoramic image of the Vancouver Stanley Cup Final in June 2011, provided by the Vancouver Gigapixel Project, allows the tagging of individuals' faces over a distance of the far away back end of the Vancouver Canucks Fan crowd. Information on the high-res image and its tagging functionalities are available online at:
http://www.gigapixel.com/image/gigapan-canucks-g7.html. Also see the article "Technology Is Our Friend ... Except When It Isn't" by James Fallows, published at

A couple of months back, a CCTV camera introduced at an open spot caught a couple having intercourse. For another situation, a camera caught a couple kissing in the Delhi metro. The recording of both discovered their way to the web.

"In the present occasions, CCTVs are a flat out must. In this way, enactment should find some kind of harmony among protection & security," Duggal includes point by point rules are required the obligations of CCTV camera proprietors to the extent due constancy is worried, as they are named go-betweens under the IT Act. Likewise, the degree of the risk in instances of break of delicate data or film must be indicated.

The security law, which has been at the drafting stage since the previous five years, plans to have a different section on reconnaissance, specifying the rules & regulations for CCTV cameras. Abraham says, "The section of a protection Bill by the Parliament will guarantee globally acknowledged security standards will be executed in the letter of the Indian law." This will guarantee residents have rights that they can implement against companies & government organizations utilizing CCTV cameras, includes Abraham, a functioning member in confining a few drafts of the security law.

JUSTIFICATION OF LAW FOR SURVELLIANCE

Not just have the security ramifications of video reconnaissance frameworks not been enough considered, however neighbourhood governments have additionally neglected to look at the genuine viability of cameras. The essential implied[39] basis by law requirement for arrangement what's more, development of camera frameworks has been decrease of wrongdoing, going from fierce wrongdoing to unlawful dumping. Optionally, authorities have likewise looked to legitimize camera use as a methods for recording proof of crime to be utilized in future arraignment. Be that

as it may, neither of these avocations have been bolstered by proof or assessment.

REDUCTION IN CRIMES:

theAtlantic.com August 27th 2011, and pointing out the dangers of such facial recognition in crowd sceneries to the exercise of civil liberties in public, available at:

http://www.theatlantic.com/technology/archive/2011/08/technology-is-our-friend-except-when-

itisnt/244233"1st October, 2019, 12:30

[39] An exemplary description of possible techniques was made by Yisu Zhaos thesis submitted to the Faculty of Graduate and Postdoctoral Studies, Ottawa-Carleton Institute for Computer Science, "Human Emotion Recognition from Body Language of the Head using Soft Computing Techniques",1st October, 2019, 12:50 available at: ruor.uottawa.ca/en/bitstream/handle/10393/23468/Zhao_Yisu_2012_thesis.pdf?sequence=1

The main avocation given by law authorization (and others) for the production of video reconnaissance projects is to diminish wrongdoing through prevention. From Oakley where Police Chief Chris Thorsen has asserted that the establishment of two cameras in that little network will fill in as a "power multiplier" with "impediment esteem," to bigger urban areas, for example, San Francisco where cameras are being introduced in horror regions in light of a heightening manslaughter rate, cameras are being touted as a wrongdoing avoidance tool. While it might appear to be instinctive to strategy producers that video reconnaissance cameras will decrease wrongdoing, various investigations show the inverse.

In Britain[40] where camera (CCTV) frameworks have been set up for near a decade, criminologists have directed various investigations to audit their real sway. One early survey was led by the Scottish Central Research Unit and assessed wrongdoing measurements going before and following the organization of observation cameras in Glasgow, Scotland. There, scientists discovered cameras had little sway on wrongdoing finding decreases in wrongdoing not any more noteworthy than those in control territories without the camera areas.

IT HELPS IN PROSECUTION & APPREHENSION

Law requirement elements additionally legitimize cameras by guaranteeing that they will catch proof of crime and the recording can be utilized in worry or in future criminal arraignment. For instance, the London police profoundly announced the job of the CCTV cameras in recognizing the psychological militants associated with bombarding the metro in 2005. In spite of the fact that cameras without a doubt catch some data that can be of future use, in numerous ways, the job of cameras has been exceptionally restricted[41], frequently just giving a few help to continuous examinations. While we are ignorant of any thorough examinations demonstrating the degree to which cameras positively affect wrongdoing freedom and arraignment, some restricted proof proposes their effect in such manner may not

[40] Since this document is meant to give only an overview of the current and upcoming technical possibilities in the field of CCTV, a more detailed description and effectiveness analysis of the individual functionalities is unfortunately out of scope. However, the most interesting algorithms, namely object detection, object tracking, object classification, event detection, and route reconstruction were already described in detail within the ADDPRIV Deliverable 2.1 (pp. 45 ff.). Most of these algorithms are still subject to further research in this field, thus it is to be expected that even more advanced and effective techniques will be available in near future. 21 Francine Prokoski, "History, Current Status, and Future of Infrared Identification", published in 2000 in IEEE Computer Society, Computer Vision beyond the Visible Spectrum: Methods and Applications, pp. 5-14, 30th September, 2019, 21:54 marathon.cse.usf.edu/~sarkar/biometrics/papers/IRSummary.pdf"

[41] MIT News web magazine, article by David L. Chandler, May 25th 2012, "Is that smile real or fake? A computerized system developed at MIT can tell the difference between smiles of joy and smiles of frustration." 5th October, 2019, 23:09, http://web.mit.edu/newsoffice/2012/smile-detector-0525.html

be as critical true to form. Further, the nature of the pictures gathered and the plausibility of computerized film being altered or corrupted may make it hard to use as proof in a indictment.

In the first place, some proof proposes that the impact of cameras on law requirement's capacity to clear wrongdoings isn't fundamentally helped by the nearness of video reconnaissance cameras. The Glasgow study referred to above[42], for instance, found that "the cameras showed up to have little impact on the unmistakable up rates for wrongdoings and offenses for the most part. Looking at insights when establishment of the cameras, the reasonable up rate expanded somewhat from 62% to 64%. When these figures were balanced for general patterns, in any case, the examine investigators reason that the unmistakable up rate tumbled from 64% to 60%.

Second, while some extra violations will unquestionably be caught on film, the degree to which cameras help law requirement is frequently enormously overestimated. In Maryland, for instance, a representative for the State Attorney's Office told columnists for the Washington Times, that the workplace has not "observed them to be a helpful apparatus to investigator they're useful for incidental proof, yet it certainly isn't confirm that discovery is helpful to convict someone of a wrongdoing.

Eventually, the security fight over the best possible use and extent of facial acknowledgment reconnaissance will happen in the city, not in the courts[43]. In London, for instance, the Metropolitan Police have tried different things with facial acknowledgment innovation, with blended outcomes. Prior to revealing the new innovation[44], the police expressed that individuals who canvassed their face in territories where there were cameras would not be halted for suspicious conduct.

However, that was not really the case once the innovation was at that point set up. In one prominent case, a man[45] who was halted for covering his face was later fined by the police in

[42] David Talbot, "Wiping Away Your Siri 'Fingerprint'", MIT Technology Review, September 28th 2019, 12:32 http://www.technologyreview.com/news/428053/wiping-away-your-siri-fingerprint

[43] Currently, IBM is testing a new traffic-management technology in a pilot programme in Lyon, France, using big data to achieve a better performance of large data processing in traffic surveillance areas, Wired.com article by Doug Newcomb, published November 21st 2012, seen at 28th September, 2019, 14:56 "How Big Data Will Ease Your Commute", www.wired.com/autopia/2012/11/big-data-commute

[44] This leads to intensified efforts by vendors to provide improved software able to centralize different alarm sources and filter out relevant events needing human intervention; see for example the article in the Security Middle East Magazine issue 65 March/April 2012, titled "Improving situational awareness", 1st October 2019, 17:50 http://www.securitymiddleeastmagazine.com/features/view/32

[45] This is for example a weakness of the aforementioned "automatic action recognition" functionality, which predetermines certain actions of individuals and thus is not yet able to ascertain unforeseen activities of

the wake of swearing and getting to be threatening. Obviously, you can see this conduct in one of two different ways – as the activities of a "liable" individual who was appropriately halted and kept by the police for covering his face, or as the insulted activities of" a "blameless" individual who was inappropriately halted and confined on an absurd charge.

Unmistakably, there is a hazy dark line here. When do you stop somebody essentially in light of the fact that they are attempting to keep up their protection?[46] London cops were advised to "use judgment" when halting individuals who keep away from the cameras, yet doesn't that suggest that specific sorts of individuals –, for example, youngsters of shading – will be halted more regularly than others?

An opportunity to manage another innovation is at the very start, and not after it has turned out to be so dug in and imbued that disposing of it would appear to be pointlessly mind boggling.

That is the reason the present minute is so significant. Facial acknowledgment frameworks are presently utilized in air terminals and at fringe intersections by movement and traditions authorization experts. They are utilized as group control apparatuses in tyrant countries. Furthermore, they are utilized by informal communities. It's currently similarly as normal for somebody to login to their computerized gadget with their face all things considered with their unique mark. So we truly are at a tipping moment that it comes to choosing how to manage cutting edge observation frameworks that utilization our face as the essential type of ID – on the off chance that we hold up a couple of more years, it may be past the point where it is possible to take care of business.

individuals, see the article by Adi Robertson, "Military-backed surveillance prototype can read people's actions on video" 1st September, 2019, 13:09.

[46] Such failures caused by the false analysis of camera data is described on the basis of a

case study by Alex Stedmon in his article "The camera never lies, or does it? The dangers of taking CCTV surveillance at face value and the importance of human factors", Surveillance & Society, vol. 9, no 3 (2012), "Urban Surveillance", http://library.queensu.ca/ojs/index.php/surveillance-and-society/article/view/4192/4194; see also the article by SA Mathieson and Rob Evans for The Guardian, "Roadside cameras suffer from large gaps in coverage, police admit", September 27th 2019, http://www.guardian.co.uk/uk/2012/aug/27/police-number-plate-cameras-networkpatchy

CONCLUSION & RECOMMENDATIONS

Since Countries have different types of laws governing them, so it is safe to assume that their approach towards issue like privacy and that too in the Big Data Age will be different. Since it is a modern problem, most of them do not have laid down procedures set up for implementation with regard to privacy. Moreover it is seen to be an alarming state when a citizens' data or sensitive personal information being tracked by the government along with big tech companies. It is human tendency that even if a company promises to safeguard your sensitive data with them and assures that it will not leak it, we know that there are hackers that can hack the softwares of such companies and steal all the data, or even the company itself can sell such data at whatever price they want to. It is also seen the not only MNC's, but also service providers do not maintain privacy on multiple platforms which are online. But, at the same time there are some countries whose policies regarding data protection and privacy is plausible. Though, rule of law being implemented to such policies is still a rarity.

1. The government must provide with a clear framework of guidelines which imbibe collecting, monitor, storing, and ownership of data, for MNC's, Tech companies and various others involved in collection of such data.
2. There must be a set of policies and counter measures which will protect the people and their data from cyber risks and misuse by top level officials. The laws concerning privacy should protect a user's passwords, fingerprints, medical history, etc. moreover it should ask for an express consent of the user before collecting the data. If a company collects data of a user for a certain usage, then the data must be deleted after the said use.
3. State and non state actors must be controlled of their data collection by bodies such as the TRAI (Telecom Regulatory Authority of India)
4. The public at large should be allowed to give their opinion as to how the government can protect and improve such data and privacy protection policies.
5. If national security concern arises, then a judicial authority must give an authorization to access any information in data canters.
6. Laws to be made for the protection of data centre's digital safeguards.
7. Technology like PET (Privacy Enhancing Technology) must be allowed to be used by users so that it becomes their choice to remain unknown or to disclose their location.
8. All data which is being collected by the state in the facade of national security should be immediately put to a stop until laws and regulations are made for the same.
9. A before-hand consent or authorization from the particular authority must be taken, and

only after that should the data be collected.

10. An express and informed consent from users should be taken for collecting their data.
11. Most importantly, awareness of such privacy and data importance must be given number one priority. The citizens should what are the outcome of their data being leaked or taken which consent, and how it could harm them. The users must be educated.

REFERENCES

- CCTV Surveillance in Public Spaces of Delhi: Exploring the Perspectives of Youth visiting Malls and Delhi Metro, By Sanchita Hasija and Shruti Nagpal, IOSR Journal Of Humanities And Social Science (IOSR-JHSS) Volume 23, Issue 12.
- Agarwal, Surabhi, "Violation of privacy through CCTV cameras rampant, say experts." Business Standard, New Delhi, April 4,2015, http://www.business-standard.com/article/currentaffairs/violation-of-privacy-through-cctv-cameras- rampant-say-experts-115040400775_1.html.
- https://indiankanoon.org/doc/112223167/, Section 66E in The Information Technology Act, 2000, India Kanoon.
- M. K.Kakhani, S. Kakhani and S. R.Biradar, Research issues in big data analytics, International Journal of Application or Innovation in Engineering & Management, 2(8) (2015), pp.228-232.
- A. Gandomi and M. Haider, Beyond the hype: Big data concepts, methods, and analytics, International Journal of Information Management, 35(2) (2015), pp.137-144.
- Ninny Bhogal, Shaveta Jain," A Review on Big Data Security and Handling", International Research Based Journal, Vol(6)-Issue(1) , ISSN 2348-1943, March,11, 2017.
- Mohammed S.Al-Kahtani," Security and Privacy in Big Data", International Journal of Computer Engineering and Information Technology, VOL. 9, NO. 2, E-ISSN 2412-8856, February 2017.
- Mr. Shrikant Rangrao Kadam, Vijaykumar Patil, "Review on Big Data Security in Hadoop", International Research Journal of Engineering and Technology (IRJET), eISSN: 2395 -0056, Volume: 04 Issue: 01, pISSN: 2395-0072, Jan -2017.
- J.L. Joneston Dhas, S. Maria Celestin Vigila and C. Ezhil Star," A Framework on Security and Privacy-Preserving for Storage of Health Information Using Big Data", IJCTA, 10(03), pp. 91-100, International Science Press, 2017.
- R.Kalaivani," Security Perspectives on Deployment of Big Data using Cloud: A Survey", International Journal of Advanced Networking & Applications (IJANA), Volume: 08, Issue: 05 Pages: 5-9, Special Issue, 2017.
- Vinod B. Bharat, Pramod B. Deshmukh, Laxmikant S. Malphedwar, P. Malathi and Nilesh N. Wani, "Big Data and Database Security", IJCTA, 10(8), pp. 517-528 ISSN: 0974-5572, International Science Press, 2017.
- Trupti V. Pathrabe, "Survey on Security Issues of Growing Technology: Big Data", IJIRST, National Conference on Latest Trends in Networking and Cyber Security, March 2017.
- . Saetnan, Lomell, Wiecek(2004), Controlling CCTV in Public Spaces: Is Privacy the (Only) Issue? Reflections on Norwegian and Danish observations, Surveillance and Society,http://www.surveillanceand-society.org/articles2(2)/controlling.pdf
- https://www.ifsecglobal.com/role-cctv-

cameras-public-privacy-protection/ "Role of CCTV Cameras: Public, Privacy and Protection", IFSEC Global, January 1, 2014

- K.P.Maheswari, P.Ramya, S.Nirmala Devi," Study and Analyses of SecurityLevels in Big Data and Cloud Computing", International on Recent Trends in Engineering Science, Humanities and Management, February 2017.
- Z. Hongjun, H. Wenning, H. Dengchao and M. Yuxing, Survey of research on information security in big data, Congresso da sociedada Brasileira de Computacao, 2014, pp.1-6.
- O. Y. Al-Jarrah, P. D. Yoo, S. Muhaidat, G. K. Karagiannidis and K. Taha, Efficient machine learning for big data: A review, Big Data Research, 2(3) (2015), pp.87-93
- C. L. Philip, Q. Chen and C. Y. Zhang, Data-intensive applications, challenges, techniques and technologies: A survey on big data, Information Sciences, 275 (2014), pp.314-347.

*****