Delhi Metropolitan Education
Affiliated to GGSIP University, New Delhi & Approved by Bar Council of India

RESEARCH ARTICLE
doi: 10.53361/dmejl.v5i02.04

Government Monitoring with The use of Upcoming Technologies and The Right to Privacy: An Analysis

B. Mathanachandiran[1], Ratheesh Kumar[2]

[1]*Assistant Professor- VISTAS, Chennai.*
[2]*V.V Associate Professor and HOD-VISTAS Chennai.*

Abstract

In the modern world, in order to receive services from the government and non-governmental organizations, a person must provide them access to his personal information. This disclosure of private data only extends to the date of his birth. A birth certificate requires the following information to be disclosed: name, location and date of birth, parent names and ages, etc. Both public and private educational institutions demand the same personal information in order to admit students. The government requires many identities of verification before granting him a driver's license and voter card. In order to be eligible for subsidized food or other services, an individual must provide their name, address, picture, fingerprint, and iris scan. and other biological traits. Property ownership or possession also necessitates the government documentation of the party's identities and other information. An arrested Even in minor cases, a person or detainee may be required to provide his personal details such as his fingerprints, face features, blood type, gene sample, etc. Additionally, personal data must be provided for income tax reasons, banking transactions, etc. Sometimes, a deceased individual can only rest in peace if he has an identification card that has been approved by the government. Furthermore, the deceased individual lives on in the digital realm since personal data may be kept on computers indefinitely. Private service companies retain more personal data about each individual than do government records. A person interacts with private service providers more often than with governmental organizations. An individual divulges his personal information to private service providers as part of his daily routine in order to do a variety of tasks, such as watching television, using a smartphone, browsing the internet, shopping online or off, traveling, touring, social networking, eating, drinking, writing, speaking, and so on. Private service providers save a lot of personal data and utilize it for their own business endeavours. People, on the other hand, virtually ever know why such vast amounts of data have been gathered or whether they will be utilized for the intended goals. Throughout history, both public and private organizations have gathered and utilized people's personal data for their intended uses.

ARTICLE INFO

Correspondence:
lawbmc696@gmail.com
V.V Associate Professor and HOD-VISTAS Chennai.

Dates:
Received: 19-07-2024
Accepted: 19-08-2024
Published: 30-12-2024

Keywords:
Government, Information, Data, Records

How to Cite:
Mathanachandiran, B., Kumar, R. (2024) Government Monitoring with The use of Upcoming Technologies and The Right to Privacy: An Analysis. DME Journal of Law, 5(2), 40-46. doi: 10.53361/dmejl.v5i02.04

Introduction

In the modern world, in order to receive services from the government and non-governmental organizations, a person must provide them access to his personal information. This disclosure of private data only extends to the date of his birth. A birth certificate requires the following information to be disclosed:

DME
Journal of Law

name, location and date of birth, parent names and ages, etc. Both public and private educational institutions demand the same personal information in order to admit students.The government requires many identities of verification before granting him a driver's license and voter card. In order to be eligible for subsidized food or other services, an individual must provide their name, address, picture, fingerprint, and iris scan. and other biological traits. Property ownership or possession also necessitates the government documentation of the parties' identities and other information. An arrested Even in minor cases, a person or detainee may be required to provide his personal details such as his fingerprints, face features, blood type, gene sample, etc.Additionally, personal data must be provided for income tax reasons, banking transactions, etc. Sometimes, a deceased individual can only rest in peace if he has an identification card that has been approved by the government. Furthermore, the deceased individual lives on in the digital realm since personal data may be kept on computers indefinitely. Private service companies retain more personal data about each individual than do government records. A person interacts with private service providers more often than with governmental organizations. An individual divulges his personal information to private service providers as part of his daily routine in order to do a variety of tasks, such as watching television, using a smartphone, browsing the internet, shopping online or off, traveling, touring, social networking, eating, drinking, writing, speaking, and so on. Private service providers save a lot of personal data and utilize it for their own business endeavours. People, on the other hand, virtually ever know why such vast amounts of data have been gathered or whether they will be utilized for the intended goals. Throughout history, both public and private organizations have gathered and utilized people's personal data for their intended uses. Computer technology has made it possible for these organizations to store and handle data more effectively than in the past.[1]Finding useful information among the vast volumes of data kept in databases, data warehouses, and other information repositories is a technique known as data mining in the context of computer technology.[2]

Camera Technology and Monitoring by The Government

The global increase in crime and terrorism has granted governments everywhere complete authority to erect as many closed-circuit television (CCTV) cameras as they like. Following terrorist attacks on the city in the early 1990s employing truck explosives, the London authorities were among the first to implement broad closed-circuit television (CCTV)surveillance. The number of cameras in the city increased by 72% between 2012 and 2015, accounting for one-third of all cameras in the United Kingdom.The government deploys audio-video cameras in public areas to deter crime. Camera recordings are used by security investigators to investigate and solve crimes. The technology of audio-video cameras is important for safety, quality assurance, fire safety, security, and other reasons. Furthermore, there could be obvious advantages for both the general public and employees when cameras are placed in dangerous industrial sites or dim, exposed public spaces.During the assault on September 11, 2001, video cameras employing other instruments saved countless lives.[3]They might easily fit into tiny robotic insects, birds, wasps, bees, ants, house flies, mosquitoes, and other creatures of this size. To do aerial surveillance, miniature cameras can also be installed in satellites, drones, aircraft, and other vehicles. It is also capable of remote control. On the other hand, there are countless websites that provide intimate, personal, and even pornographic video footage taken by covert cameras. Covert cameras are recording people's most intimate moments and posting them on websites. Everything is carried out without their awareness or approval.[4]This report from Big Brother Watch, released on Tuesday, warns that facial recognition technology turns innocent British citizens into "walking ID cards." It claims that the

1 Daniel J. Solove, Privacy, Information and Technology, 160 (2006).

2 Jiawei Han and Micheline Kamber, Data Mining: Concepts and Techniques, 7 (2010).

3 Herman Kruegle, CCTV Surveillance: Analog and Digital Video Practices and Technology, 1 (2007).

4 J.K. Peterson, Handbook of Surveillance Technologies, 476 (2012).

technology, which involves computer databases of faces linked to CCTV and other cameras, was used by the Metropolitan police to spot people on a mental health watch list at the 2017 Remembrance Sunday event in London. Police attempts to use cameras linked to databases to recognize people from their face are failing, with the wrong person picked out nine times out of ten, the report claims. In addition, police in South Wales used it during protests against an arms fair. They also intend to use it at music festivals and other events. Some in the police community view facial recognition as the next big step towards enforcing the law, similar to the revolution brought about by advances in DNA analysis. Privacy campaigners view it as the next major battleground for civil liberties, as the state effectively demands that some privacy be given up in exchange for increased security. However, the Big Brother Watch report states that the benefits are not yet realized because the technology is unreliable.Beatrice von Silva-Tarouca Larsen argued that CCTV surveillance is only allowed when there is a "comprehensively documented and significant criminal threat" at a specific location. She stated, "To protect anonymity against unwarranted intrusions, it is imperative to assess the risks. The mere possibility of crime occurring cannot provide sufficient grounds for public CCTV, or there would hardly ever be a reason to install it." The agencies are using CCTV surveillance extensively, as if all of the traditional modes of surveillance have failed. Full privacy impact assessments are required before any installation.

Technology and Privacy with Smart Phones

One of a person's most private documents these days is their smartphone. Through the internet, phones may connect to the outside world. A mobile phone contains personal data about its owner as well as friends and family. Private photos and videos, messages, call and location logs, online and chat histories, past purchases, bank account information, company details, salary records, and more are all included in the personal data. Users may still be able to retrieve erased data from their phone's databases by searching through the databases of social networking sites, app developers, telecom or internet service providers, and other organizations. In exchange for offering their services to the subscriber or user, telecom service providers, internet service providers, and app developers obtain total access to the user's phone.WhatsApp was found guilty in 2013 of violating global privacy regulations due to its practice of compelling users to give it access to their whole address book. It keeps all of that data arbitrarily, which means that over the years, millions of non-consenting non-users have had their data exposed.The makers of mobile devices, software creators, telecom companies, and other service providers are all privy to every detail regarding their customers. Furthermore, these information storekeepers are required by harsh laws of today to offer simple access to the datasets held by the governments. In accordance with these laws, the governments are authorized to examine and intercept any correspondence or data in order to prevent any criminal activity; to safeguard state security; to preserve the sovereignty of state, and so forth. The due process provision mandates that they provide proof of reason prior to any such intercession. But law enforcement would constantly attempt to avoid this need when they are aware that their unauthorized access and interception would rarely be tracked down.This phenomenon can be attributed to the ongoing storage and transmission of people' personal information. An individual is unaware of the ways in which his personal information has been exploited. His data is dispersed around the internet. Because they are aware that they can obtain a search warrant quickly and without being tracked down, law enforcement agencies don't feel the need to obtain one.[5]Mobile phone hacking has grown commonplace for both government and private organizations. Malware known as "ransomware" encrypts a computer's data and prevents access, then demands payment to unlock it. This software has the ability to blackmail anyone. Governments and large corporations have already been compromised.In the San Bernardino case, the government of the United States hired a hacker (despite careful caution) to unlock the attacker's iPhone encryption key.

5 See Glenn Greenwald, No Place to Hide, (2014).

Furthermore, it was carried out without a judge's approval, which is against the US Constitution's due process and Fourth Amendment provisions.

Technology for Satellite Surveillance

Since the conclusion of the Cold War, the United States and other nations have used satellite surveillance. Numerous private and commercial entities, such as EarthWatch, Motorola, and Boeing, are the owners of these monitoring satellites. These businesses assist governments in mapping every aspect of the planet. These businesses sell satellite imagery to governments. The photos were utilized by the US military to conduct operations in Syria, Afghanistan, Iraq, and other countries. Using images from commercial satellites is government policy. Anywhere on Earth, a satellite can identify things as tiny as one meter (3.28 ft). Individual trees, cars, road networks, and homes are visible to viewers. QuickBird, a satellite launched by DigitalGlobe in 2001, can provide photos as small as two feet (0.61 meters). With their next-generation WorldView 1 satellite, due to launch in mid-2007, and their WorldView 2 satellite, expected to launch in late-2008, DigitalGlobe is now focusing on boosting resolution and collection capacity. With just an address or a search, anyone may view a map in satellite format by downloading Google Earth for free.The business provides two enhanced versions of Google Earth that include data input capabilities for more sophisticated applications and Global Positioning System (GPS) technology for an extra charge. In a more constrained version, the satellite option was first made available through Google Maps, the company's online mapping service. Satellite picture access has improved in convenience and accessibility. Anyone with an internet connection may view satellite pictures on their phone.The global positioning location patterns of each individual may be read by computer software. A viewer may learn anything about a person by just clicking on their location, as satellite imaging software allows any personal information about an individual to linked. Similarly, these satellite imaging sites display information of any found object or area.More sophisticated and advanced satellites have been constructed by two businesses, one from America and the other from Finland, to scan the whole planet regardless of the weather, amount of daylight, or cloud cover. With current technology, these sophisticated satellites can now visit almost any location on Earth up to once per hour. The technology's extremely low cost is another of its features. Seeing satellite imagery would attract more interested buyers.However, it also brings up the risk of privacy invasion. Neil Richards stated, "Unregulated government access is probably what worries me the most about observational technology." Prior to the widespread use of new technologies, it is crucial that we have open discussions to clarify our values and the values we wish to see included into them. In the end, power comes from knowledge. This has been known for ages. Furthermore, information-driven digital technology offers even greater power. According to Ray Purdy, a specialist in satellite law at University College London, the majority of satellites are owned by businesses, so you may purchase the pictures if you're wealthy. Thus, anybody can survey anybody. The main point is that there was no privacy debate during its development, and once technology is released, it is difficult to revert. Purdy desires a thorough public deliberation and the establishment of guidelines for the use of satellites in criminal cases in order to prevent their introduction covertly.

Biometric Technology

Biometric refers to bodily measurement. In order to confirm a person's identity, biometric technology collects, measures, and processes that person's particular or distinctive human features.[6]The analysis of behavioural traits such as writing or signatures, voice patterns, facial expressions, and so on is used for identification. Recently, brain patterns and heart rhythms have been studied as

6 Biometric technologies imply that unique or distinctive human characteristics of a person are collected, measured and stored for the automated verification of a claim made by that person or the identification of that person. Els J. Kindt, *Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis*, 19 (2013).

biometric identification methods.[7]The capabilities of biometric technology are being used by both public and commercial organizations to meet their needs. As previously noted, radio chips and biometric technologies are used by public and private companies, such as schools, colleges, and universities, to guarantee that their staff members attend work on a regular basis. In order to give account holders secure and effective banking services, banks want biometric information. Hospitals use biometric technologies for treating their patients. To stop fraud, insurance firms use biometrics.In India, possessing an Aadhar carda unique identity number that carries the holder's physical characteristics, such as a fingerprint, iris scan, and facial imagehas become mandatory for all access to public and private services. If a person doesn't have an Aadhar card or their biometrics don't match the government's database, they frequently won't be able to receive even subsidized food items that are recognized under the public distribution scheme.The primary concern in this case is the security and accuracy of the biometric technology; however, the system's flaws give rise to concerns about both security and privacy. In the modern world, there is a serious risk when a person must interact or transact with the primary biometric technology usersgovernment agencies, commercial entities, private employers, educational institutions, banks, retail centers, and the likein order to obtain necessities of life.

DNA Database and Right to Rivacy

The government and private sectors collect Deoxyribonucleic Acid (DNA) samples for a variety of reasons, such as identity, criminal investigations, medical treatment, medical research, employment, insurance policies, etc. It is said that the effect of genes is inherited by subsequent generations. According on what is known about genetic testing, it can identify future characteristics and behaviour of a person while disregarding the psychological and sociological aspects of human body. Consequently, if an individual has particular genes that have been connected to with some criminal activity, segregation throughout society is a real possibility. In addition, the authorities would be keeping a closer eye on this individual and could suspect him of a crime even if he hasn't done any. Under such circumstances, it would be considered a breach of fundamental criminal law principles, such as the right to silence, the assumption of innocence, a fair trial, etc. Likewise, in the unwholesomely cutthroat global marketplace, businesses would subject their staff members to DNA testing. It should come as no surprise that employers will only select genes with the most potential to advance the company.It has been noted that these Deoxyribonucleic Acid (DNA) profiles are kept on file by law enforcement organizations indefinitely. Even when the suspects and convicted are found not guilty, they continue to propagate false information. In S. and Marper v. United Kingdom[8], the European Court of Human Rights took this into consideration.Currently, computerized databank of each individual's Deoxyribonucleic Acid (DNA) profile has also been accessible to the private entities like insurance companies, employers, schools, adoption agencies, etc., which are utilizing it for their own reasons. Due to a genetic illness, ancestry, or other genetic defect, an individual may not be eligible for adoption, health treatment, or other benefits.

Technology of Brain Reading

Many technological innovations have been made by scientists to track and regulate brain activity. Consumer Based electroencephalography (EEG) headset is capable of assessing a mental state. It has the ability to discern whether or not a person is in a calm frame of mind.

In a similar vein, brain perception, memory, emotion, and movement may all be ascertained with functional magnetic resonance imaging (fMRI) technology. A recent development in cognitive technology is optogenetics. Optogentics is the use of genetic engineering and light to regulate a neuron's activity. Scientists were able to successfully manipulate the brains of mice they used in tests.In their trials, the scientists also demonstrated how the cockroach followed their instructions for movement.

7 See Els J. Kindt, Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis, (2013).

8 (2009) 48 EHRR 50.

Moreover, brain implants at the micro level are being utilized to read neural activity. A network of neurograinswireless brain implantswould be able to detect neural activity and transmit it to an outside computer for analysis. "neurograins." Every neurograin is made up of a radio frequency (RF) energy-harvesting chip that powers an electrode that detects voltage spikes from individual neurons and facilitates wireless communication. The radio frequency (RF) power is supplied by an antenna placed outside the skull, which also transmits data to and receives it from the implants.Users with brain chips would be able to communicate with computers, the internet, and mobile devices solely using their brain waves by 2020.[9]The advancement of neurological science has the benefit of helping patients who are in need of psychological support. Furthermore, it's critical to provide people with these tools so they may take charge of their physical and emotional well-being. However, one drawback of technology is that it may also be utilized by anybody to violate someone's mental privacy. It can be used by private service providers for their own profit-making endeavors. Employers in China are using brain reading technology to ascertain their employees' emotional states. Similarly, the totalitarian governments would use it for their political ends. While the nature of criminal law and its fundamental principles shield people's ideas and fantasies from prying eyes, unwanted attention, or legal repercussions, "brain-reading technologies" have the potential to erode this type of mental privacy. Users of brain-reading technology would apply it for their own goals, which may be influenced by preconceived notions they already have about a person or group of people.Opponents of the despotic administrations would even face consequences for intellectual crimes. Andrea Lavazza notes, "if Nazi criminals, like other evil people in the history of humanity, had come to realize that their victims could find great comfort in thoughts concealed within their minds, they would have tried to stop this by all means. We may, however, be living at a time where this is feasible."With commercialization of BCI (brain-computer interfaces) technologies moving forward, connecting human brains directly to the internet, portends a chilling reality," stated Elliot D. Cohen. "This puts a government in possession of the means to manipulate and control these brains."[10]Cohen issued a warning, stating that "the idea of" future access to "private thoughts of human beings" by the already operating mass surveillance programs, which are carried out without any legal or judicial supervision, would be problematic. Democracy and freedom will end up becoming meaningless ideals.

Surveillance of Artificial Intelligence

Because the artificial intelligence machine has access to all of the world's combined datasets, scientists and professionals assert that it provides the best logical solution to a given problem. It is entirely capable of utilizing every piece of technology now in use on Earth to do this. It is also capable of carrying out the choice it made based on the rational response. Artificial neural networks, evolutionary computation, clustering, data mining, and pattern recognition are just a few of the methods that artificial intelligence operates.Governments, health scientists, marketers, engineers, pharmaceutical corporations, and others are using these smart technologies for a variety of goals. Artificial intelligence holds unparalleled potential to alleviate societal injustices and suffering on a broad scale, providing policymakers with the political will to act in the public interest. With the artificial intelligence algorithm, both the vendor and the buyer may gain. Consumers would be suggested with the greatest selections of items. Artificial intelligence safeguards businesses and customers against fraud of any form. The greatest defence against such intelligent technology incursions against an individual's right to privacy would be a smart house. The authorities can get assistance from artificial intelligence in stopping and investigating crimes. The police may be alerted before any legal violations.Nevertheless,

9 Sharon Gaudin, "Intel: Chips in brains will control computers by 2020," Computerworld, November 19, 2009. Cited in Elliot D. Cohen, Technology of Oppression: Preserving Freedom and Dignity in an Age of Mass, Warrantless Surveillance, 101 (2014).

10 Elliot D. Cohen, Technology of Oppression: Preserving Freedom and Dignity in an Age of Mass, Warrantless Surveillance, 104 (2014).

the entire fabric of global civilization might be destroyed by the improper application of artificial intelligence. The usage of it and its intended purpose are determining factors. If it is built on the prevailing biases in the community or if its entire concept is according to the unlawful ideas, the individuals who really hold the planet would be under the control of artificial intelligence. They would rule the entire planet. Based on their own irrational and whimsy. Many countries make use of artificial information to execute their extensive monitoring schemes. The goal of totalitarian governments is to place everyone under observation. They desire to read and document each and every information about a person. Using artificial intelligence algorithms, the autocrats or the powerful organisations try to determine the mental health of the humans by only scanning their expression on the face. And if they come across somebody who disagrees with them or opposes their goals, they would endeavour to eradicate such individual by persecuting or punishing him. This is the ideal illustration of how a government is purposefully use AI to conduct racial profiling. China's rapidly growing networks of surveillance cameras are equipped with face recognition technology that only searches for Uighurs based on their appearance and records their arrivals and departures for further inspection and evaluation. According to experts, the use of algorithms has made it relatively simple to categorize people according to their race or ethnicity.Tenants in New York are extremely alarmed by the landlords' attempt to obtain their biometric data and install a facial recognition system in order to gain entry to certain areas of the buildings. Their resistance to the installation is evident. Additionally, they are concerned that a third party may have access to their biometric data. According to Alvaro Bedoya, the founding director of Georgetown Law's Center on Privacy & Technology, monitoring a resident's arrival and departure from their building can disclose a variety of details, such as their employment, their religious affiliations, and whether or not they are having extramarital affairs.The executive's employment of covert artificial intelligence methods to monitor the whole population goes against the separation of powers and the concepts of checks and balances since it leaves out the other branches of government and democratic institutions. Thus, it is necessary that it be governed by an impartial monitoring body.

Conclusion

One of the greatest methods for gathering data on the whole population is the census survey. Location specifics, identity information, sex, birthdate, age, married status, religion, caste, handicap, known languages, literacy status, characteristics of workers and non-workers, migratory characteristics, fertility particulars, etc. were among the topics covered by the 2011 Census of India.Governments gather and preserve a wide range of records on people in the current, unavoidable information era, many of which are accessible to the general public. These documents provide a variety of information types. Name, birthplace, date, parents' names and ages, and mother's maiden name are frequently revealed on birth certificates. Along with accident data, the government also keeps track of driver's license information. In a similar vein, voting records are open to the public and can reveal information about a person's political party affiliation, date of birth, email address, home address, and phone number. The Indian government collects data in order to identify its inhabitants. As identification, the Indian government recognizes passports, voter ID cards from elections, Aadhar cards, ration cards, Permanent Account Numbers (PAN) cards, and driver's licenses. Having identification makes using public and private services easier for a person. Public distribution systems, as the government says, may be carried out in a transparent and responsible way by identifying the population.