Journal of Law & Social Studies (JLSS)
Volume 3, Issue 2, pp 174-186
www.advancelrf.org

CCTV Cameras Surveillance, Data Protection & Privacy Under International Human Rights Laws

Muhammad Waqas Javed
Assistant Professor,
School of Law, Quaid-i-Azam University, Islamabad.
Email: mwjaved@qau.edu.pk.

Nazar Hussain
PhD Scholar
Email: advnazar770@gmail.com

Muhammad Arbab Maitla
Advocate High Court
Email: arbab067@hotmail.co.uk

Abstract

The study aims to find out and suggest that how equilibrium among surveillance through CCTVs, right of privacy and personal data protection regime can be maintained. With the objective in mind, it discusses the CCTVs' surveillance, its purposes, and scope of privacy in public or private domains under International Human Rights Law. It also focuses on General Data Protection Regulations, 2018 and its amplifications on CCTV surveillance.

Key words: CCTV, Surveillance, Data Protection, Privacy, Human Rights Laws

Introduction

Right of privacy is integral to all human rights and most significantly it is intertwined with dignity human dignity and right of life. All humans are at liberty to live their lives with dignity (Floridi, 2016). In case right of privacy is violated. It intrinsically operates as an attack over the right of life. This right was incorporated in Universal Declaration of Human Rights (UDHR), 1948. It was later also made part of International Covenant on Civil and Political Rights (ICCPR), 1966. Human rights Committee in its general comment No. 16 has elaborated the right of privacy in nexus with the word "unlawful" in ICCPR. However, this term has not been defined in both, UDHR or ICCPR, vital human rights treaties. Thus, it is one of the most confused concepts. Various authors have elaborated it in different senses which will be discussed in here. Further, this right has also been discussed in various regional conventions.

With the advancement of technology, this right is under more threat. Today, governments or private persons are installing CCTV systems for security or other allied purposes in public or private domains. It may pose threat to privacy (Holvast, 2019) while ignoring human rights best practices and Data Protection Regulations available either globally or regionally. It has further violated and circumscribed the right of privacy. Many a times data recorded from the system may be put on social media or abused in other ways. Before going into any further details, it is indispensable to discuss the research questions, objectives, methodology, background of right of privacy; privacy under international law, scope of privacy and surveillance in general.

Research Questions

i. *Whether or not CCTV surveillance is violative to privacy laws in International Human rights laws?*
ii. What is the scope of Data Protection Regulations and its amplifications on CCTV surveillance?
iii. Whether right of privacy is merely limited to private territory or extended to public places?

Research Object

To find how to balance between CCTVs' surveillance, right of privacy and General Data Protection Regulations, 2018. Furthermore, this paper explores the purposes of CCTV surveillances and identifies the scope of right of privacy in International Laws.

Methodology

The methodology used for the research is the qualitative approach; It also analytically and comparatively discussed tri-concepts of privacy, CCTVs' surveillance and personal data protection in the light of states' enhancing usage of CCTV surveillance for various purposes, privacy under International Human Rights law & international best practices, EU General Data Protection Regulations, 2018 and national or regional courts' decisions on issue in hand, as a primary source. While opinions of various jurists and other sources were also used as a secondary mean to conduct the instant legal research.

Privacy Background

Privacy is not a novel concept; it has base in ancient times. Most recently, concept of privacy may have its roots in a paper of Samuel W. and Louis D. B. In which they discussed right of life and its extended scope. They deliberated initially right of life was limited to various types of battery. Later, it was extended to enjoyment of life which includes "right to be alone" and to have liberty (Holvast, 2019). Thus, it gave the right of privacy an origin, and it was considered as an integral part of it. The very important paragraph concluding about privacy and significant to the instant work is as;

> *"If we are correct in this conclusion, the existing law affords a principle which may be invoked to protect the privacy of the individual from invasion either by the too enterprising press, the photographer, or the possessor of any other modern device for recording or reproducing scenes or sound".*

Under privacy any publication of these matters might not be allowed, subject to restrictions on it as a matter of public or general interest or published with consent or under privileged communication**.** Meanwhile, to take defense that the matter published was true, no malice on the part of the publisher, there are not valid defenses (Brandeis & Warren, 1890).

Today, the interpretation is even very much relevant as it relates to individual's privacy including bodily or territorial privacy and CCTV as It has given reference to 'any device recording scenes or sound'. CCTV systems are enabled to record either video and photos or sound or both. Interpreting the study with CCTV surveillance, it may be said that usage of such surveillance is allowed only for public interest or with consent of data subject. In this way, the study is a masterpiece work that might have led to incorporation right of privacy in UDHR, ICCPR and other international human rights instruments.

Privacy under International Human Rights Covenants

Privacy and Dignity

Privacy was recognized as a human right by the world community after the World War (WW) -II, before it was given constitutional protection by the states (Diggelmann, & Cleis, 2014). Right of privacy and human dignity are interconnected like two wheels connected to each other. Survival without privacy is meant to be without dignity and vice versa (Floridi, 2016). It shows the paramount significance of privacy right (Cheung, 2014).

UDHR, 1948 & ICCPR, 1966

International community while formulating the first human right document enunciated the right of privacy in it. The instrument is known as United Nations Declaration on Human Rights (UDHR), 1948. Its Article 12 states as; *"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, or to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."* This right was further recognized in International Covenant on Civil and Political Rights (ICCPR), 1966. Under Article 17 of ICCPR, right of privacy is recognized and it prohibits any illegal intrusion into it. It states that *"no one shall be subject to arbitrary or unlawful interference with his privacy, family or correspondence."*

Charter of Fundamental Human Rights of European Union

At regional level, Charter of Fundamental Human Rights of European Union under Article 7 protects the right of privacy. It states, *"It states as everyone has the right to respect for his or her private and family life, home and communications"*. For data protection, under Article 8 the Charter seeks state parties to fairly deal with the data of individual with consent of the person himself or under the laws. It envisages;

> *"(1) Everyone has the right to the protection of personal data concerning him or her; (2) Such data must be processed fairly for specified purposes and based on the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified; (3) Compliance with these rules shall be subject to control by an independent authority."*

Peck v. United Kingdom

Interpreting the right of privacy and CCTV surveillance, European Court of Human Rights (EUHR) held that such surveillance in public areas does not infringe such a right when no visual data is recorded or stored (Peck v. United Kingdom, 2003). Right of privacy may be infringed only when the footages recorded from CCTV systems are made available to the public in such a way that it causes a foreseeable injury or interference with such a right. The sole meaning of the precedent is that EU court does not prohibit installation of CCTVs or recording of it rather it makes compulsory for the installer of such system to make sure protection of the data recorded (Vermeulen, 2012). In addition, well establish principles of EU courts require tri-testing measures to be adopted for CCTVs.

Other established Principles of EUHR

According to Takis Tridimas, EUHR requires certain testing for protection of privacy and affixation of CCTV in public places. First, measure (affixation of CCTV) whether logically expected to attain the aims for which it is going to be taken, known as "*Suitability Test"*. Secondly, *"Necessity Test"* envisages testing the need of measure. It analyses other preventive measures--apart from CCTV—whether can bringing the similar outcomes. Thirdly, *"Proportionality Test"* is the most significant one. Objective followed are compared with consequences on the human rights. It means need for fulfillment of the objective must be proportionally more than the fundamental rights are being affected (Tridimas, 2006). Thus, to install CCTV at the stake of privacy under the domain of EU, such a measure must pass all three tests. Civil liberties cannot be compromised through CCTV when there is no purpose of installation of such system, other measures can fulfill such aim, and consequences are more detrimental to human right than results achieved or aim it.

HRC, General Comment 16 & Privacy

Scope of "Unlawful" or "Arbitrary" Interference

The right envisaged under Article 17 of ICCPR is guarded against "unlawful" or arbitrary interference either ensuing from the act of state or any person. While states have to enact law and take steps to prohibit interference or intrusion into privacy. In this regard, various organs of the state should take all steps to prevent the abuse of these rights which has been ignored by them. It also defines the word "unlawful" which means "no interference can take place except in cases envisaged by the law. Interference authorized by States can only take place based on law, which itself must comply with the provisions, aims and objectives of the Covenant. Whereas the word "arbitrary" extends that any interference under the law should not be contrary to the provisions or objective of the ICCPR and it should be done in rational way not exceeding the circumstance of the case. In addition, states are asked to provide information about the states' bodies or authorities empowered to allow interference into privacy as per law and in case of violation of such power, and where complaints against any violation may be made. However, HRC made it clear that such right is subject to public interest of the community (UN Human Rights Committee, 1988).

Private interest subservient to Public Interest

Thus, private life is subject to general or public interest under HRC view. This was also the view of Samuel and Louis in their article *"right of privacy"* that it is subservient to interest of the society. However, this must be done through statutes specifying the exact grounds or exigencies for which such interference is allowed (UN Human Rights Committee, 1988). It means right of privacy is not absolute rather it is conditional upon circumstance of each case. But it must be abridged in an arbitrary way, and aforesaid three tests, e.g., suitability or necessity or proportionality, should be applied to measure the value of public or private interest.

Right of Privacy and its Kinds

Definition of Privacy

Defining the term privacy may be the most cumbersome and difficult job. Definition may change due to various factors available in a society differs from other another society (Alibeigi et. al., 2019). The reason may lie from the fact that none of the conventions define privacy. This may lead to what is privacy or what is not privacy. Although HRC general comment No. 16 envisaged guidelines in this regard, it does not define what acts fall within privacy.

Most of the jurists and EU Court of HR are of the view it is not possible to given definite or exhaustive definition of right of privacy (Lukács, 2016). However, Emunel Gross, in his work, has classified the definitions of privacy in three types in a very easy and exhaustive manner. It is very an exhaustive work on right of privacy.

1) On the first instance he explains privacy on the rational of *"moral rights and claim"*. Under this kind, it is the right of individual that he determines with freedom to opt what information or data he wants to share with others and to be left alone. Simultaneously, it contains a right to live his life away from the other people. 2) Privacy may also be defined an individual's control over the dissemination of his information about himself. This information may include his person, residence, identity, and personal life affairs. 3) The third type is about *"accessibility"*. It prevents undesirable public access at three stages in life of the individual enjoying privacy; i) *"Secrecy"*, there must not be any access to the people pertaining to information concerning the individual, ii) *"Segregation"*, one's person and residence must not be available to the public, iii) *"Anonymity"*, on third stage, the physical attention of the public to individual must be with his own will (Gross, 2004). Relying upon the explanation given by him, privacy may be divided into different kinds;

Kinds of privacy

First, *"privacy of data and images"*, it comprehends to regulate the rules and regulations for controlling personal data collection and its handling. Secondly, definitions may fall within the domain of *"Bodily privacy"*. It is relating to the protection of one' self against the invasive practices without consent e.g., cavity examinations; Thirdly, *"privacy of communications"*, it involves protection and non-interference in various forms of communication including mails, telephones, mobile phones, emails and other; and Forth, *"Territorial privacy"*, an individual has protection of his location and space. It enunciates to set out the restrictions on intrusion into the houses of people and other settings for instance a person's privacy in the public places (Gutwirth et. al., 2013). Privacy may also be defined in the sense; *"the claim of an individual to determine what information about himself or herself should be known to others"* (Westin, 1967; Owsley, 2014).

Surveillance

Apart from this, Alan F. Westin Book "*Privacy and Freedoms"* is also a masterpiece and a work of its own class at the time when world was facing new technology revolution, and it is still relevant even today. For him, privacy is universal for humans as well as even for animals. Although population increase may have affected the privacy of individuals, privacy has not been as much restricted by enhancement of population as it has been curtailed by the advancement in technology, the greatest invasion of privacy. Modern devices have enabled us with spying techniques not only on human actions, but also on individual's thoughts more than ever (Westin, 1967; Owsley, 2014).

Today, regarding surveillance, the era without any doubt be called as "age of surveillance" wherein we can easily be "tracked, observed or monitored". It is immaterial the type of government in state either autocratic or democratic, states are overwhelmingly using it as a tool for various purposes (Richard, 1934). Professor David Lyon defines it as "the focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction." The definition has four facets of surveillance which provides details about the purpose of surveillance. First, it *"focuses*" on learning data of person. Secondly, it is *"systematic"*, and there is no involvement of randomness or arbitrariness. Thirdly, it can also be a "routine" which means states use it for management or executive purposes translating developed society. Lastly, it has numerous purposes (Lyon, 2007; Richard, 1934).

Kinds of Surveillance

According to Alan, three kinds of surveillance those may affect privacy. First it may disturb by listening or watching the activities or action of the person concerned. Secondly, by using coercive measure or overpowering him to reveal his thoughts and traits of personality. Third kind is named as *"reproducibility of communication"*. It is something known as recording of video or sound of the person without consent and knowledge. It implies that CCTV cameras can be affixed anywhere like in lamps or other things in public places for police surveillance. In addition, one may

affix *"directional microphone"* or likewise gadgets for recording from far away to listen and record conversation of the people. Although CCTV may have benefits in curtailment of offences, for example CCTV affixed in any lift may curb crimes and used for protection, all new devices or technologies may also have potential abuses (Westin, 1967).

Surveillance, and HRC General Comment 16

Regarding surveillance, Para No. 8 of the General Comment is very significant as it seeks prohibition on surveillance through electronic devices, the current issue in hand about CCTV surveillance. It states as;

> *"Surveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations should be prohibited"*

(United Nations Human Rights Committee, General Comment No. 16, 1988). Although HRC committee has made this observation that all form of surveillance should be prohibited against the individual as it is against right of privacy ICCPR, states are practicing the surveillance methods or procedures under the principle of national security or safety of the society in general.

CCTV and Surveillance

CCTV System

CCTV system serves for larger territories with less human involvement for surveillance, making it more feasible for security objectives. Generally, the system includes CCTV is connected to monitors having data storage capacity & access control with video display device. Whereas an all-inclusive or modern system of CCTV may contain other features i.e., security alarms may be fixed on some fence or window or any door, and capacity to detect any sort of intrusion or motion detection. Today, these systems are available with direct wire-based systems to connect camera with display monitors or Wi-Fi device transmitting air signals to connect, a wireless option, television with cameras and data storage drivers. The system has various parts which provide different functions CCTV systems have many parts with a variety of functions. Major parts of system may include cameras, data distribution wires or wi-fi device, data storage, monitoring and display devices, electricity, and lighting, apart from other. These systems have been improving day by day in every part of them (US Department of Homeland Security, 2013)**.** In addition, it may also have option to record audio of the passersby or neighbours in the surroundings.

CCTV Surveillance and its purposes

As we are living in an era of technological revolution, it may bring more threat to privacy due to evolving surveillance techniques. The states or companies or even individuals have been affixing more and more CCTV systems for purpose of security or other allied purposes in public or private domains posing threat to privacy (Holvast, 2016). It may be used for protection against crime or detection of criminals and collection of evidence. It may also be used as a street surveillance by police to prevent offences (Wastin, 1967; Agustina, & Clavell, 2011). In addition to security or law and order maintenance purpose, it may also be used for various other types i.e., workplace surveillance (Banisar, & Davies, 1999), school educational surveillance (Taylor, 2012**;** Perry-Hazan, & Birnhack, 2019), and harassment preventive purposes. It may also be used for safety of persons or property.

Rational for CCTV Surveillance & Privacy in Private or Public Situation

CCTV for Maintaining Law and Order

The most common logic given for surveillance is that it is necessary to maintain law and order, and to tackle criminal activities (Wastin, 1967; Agustina, & Clavell, 2011). It is alleged if one is not involved in unlawful activities surveillance, it should not bother the one. Surveillance in private places is totally not allowed under the human rights laws. However, there is a dispute as to surveillance in the public places. When a person uses public, privacy should not be a concern. However, human rights activists oppose this rational as it may totally be against the entire concept of privacy (Paterson, 2009).

In past, it was considered that there are limitations on right of privacy in public settings. It is alleged that surveillance is allowed in public places, and right of privacy is available only to the extent of houses or private places. To the extent of public places, only requirement of regulating the surveillance is that it should not intrude into the private affairs of the individuals. However, surveillances practices have been continuously in increase. These methods have gained impetus after the use of new technology i.e., CCTV cameras. It has advanced a reason not to limit privacy to the private domain of the people. These modern technologies or systems have created new dangers to right of privacy. It not only threatens to presumptions about personal or social privacy, but also it has diminished the randomness of the

observation course (Paterson, 2009). In the past, the private affairs of the individuals may not be noticed or seen with the naked eyes, now due to excessive use of CCTV systems, these matters may be recorded with cameras and without protection of personal date, it may intrude into privacy.

CCTV for Prevention of Crimes and Gathering of Evidence

The usage of the CCTV is riffing (Ghani, 2019). Investigating authorities around the globe have been used to use it as a tool to prevent crimes through gather of evidence. It is used for finding recognition of the criminals who committed crimes through footages or pictures taken from CCTV. These footages or pictorial evidence may also provide evidence against the persons involved in criminal activities during their trial in courts. In some states, such footages are considered as primary and substantive piece of evidence (*Scott v. Harris*, 2007). In other states, it is merely regarded as circumstantial evidence. Similarly, it may also help to finding dangerous items or weapons; for instance, any unwanted or ownerless bag containing any weapon or bomb or narcotics substance and other type of dangerous substance, in any public place i.e., park or airport etc. It is one of the reasons that CCTV surveillance is enhancing worldwide.

Supreme Court of USA in *United States v. Hester*, (1924) held that constitutional protection of privacy given to the people "in their houses, persons or papers and effects" was not available to them in "open fields". Reliance can also be placed on *Oliver v. United States*, (1984). It means that the executive authorities can even observe on private lands under the principle of "open field" in USA. Nevertheless, the most significant case in USA jurisprudence was *Katz v. United States,* (1967) it was held that privacy is integral part of 4th amendment. Without lawful warrants for search of houses, communications, or persons, no search is possible. While such warrants shall only be allowed for legal rational. It is indispensable to particularly mention the premises or person or thing which needs to be searched for purposes of warrant issuance. Significantly, it was held that privacy is not limited to private spaces rather it is available to a person who got intention to have it even in public places under the doctrine of "reasonable expectation of privacy". It is a landmark case as it declares that 4th amendment of USA Constitution protects the privacy of individual rather than of home. It states about doctrine as;

> *"The question, however, is what protection it affords to those people. Generally, as here, the answer to that question requires reference to a 'place'.... there is two-fold requirement, first that a person has exhibited an actual (subjective) expectation of privacy and,*
>
> *second, that the expectation be one that society is prepared to recognize as 'reasonable.' Thus, a man's home is, for most purposes, a place where he expects privacy, but objects, activities, or statements that he exposes to the 'plain view' of outsiders are not 'protected' because no intention to keep them to himself has been exhibited.*
>
> *On the other hand, conversations in the open would not be protected against being overheard, for the expectation of privacy under the circumstances would be unreasonable."*

Global increase in CCTV surveillance

One of the reasons in the impetus for induction of CCTV system for surveillance not only in USA but also around the globe was the 9/11 terror attacks in USA and war on terror (Doyle, et. al., Eds., 2013). Similar practices can also be seen in United Kingdom (UK) after various terrorism activities. Due to these events, CCTVs are more and more deployed in almost all spheres of places e.g., airports, bus stations, power stations other significant places. The menace of terrorism became a precursor for such expansion of CCTV extending to street surveillance of the public at large (Noris, 2012).

During 1985 to 2006, particularly in UK, there was a huge surge in CCTVs, an irrefutable fact. In 2013 as per estimate of British Security Industry Authority (BSIA), around 5.9 million CCTVs were operating; a camera for eleven persons (Barrett, 2013). It can be said without doubt that "CCTV has become a "normalized" feature of British urban life"**.** It has become universal; it is not only limited to street, but it has also been utilized for traffic control (Wood, et. al., 2006). As a matter of routine, CCTV found in public transport, educational institutions, hotels, on ways, airports, working places, hospitals, and other areas. It is well known that *"citizens of urban Britain are watched over from cradle to grave"* (Wood, et. al., 2006), as in EU or perhaps of the world, UK has been one of the most surveilled country (Edwards, 2005). However, such violation of privacy rights has not been regarded as valid by The European Commission on Human Rights when government released footage of suicide attempt of an individual and considered it as totally in violation of Section 8 of Human Rights Act (Peck v. United Kingdom, 2003).

CCTV surveillance is widely used in Britain as there is lack of privacy and less constitutional shield against such rise in CCTV. During 1990s, UK government spent millions of pounds to develop surveillance systems at local levels. Similar is the trend worldwide; such progress may vary country to country. However, countries like Denmark or Canada got strong protection regimes of privacy data. Similarly, Germany —despite having totalitarian history— also has constitutional safeguards against CCTV surveillance; thus, it has less expansion of CCTVs. Norway situation is in no way different from Germany (Hempel, & Eric, (n.d)). In Africa or Asia such pattern differs, and expansion of CCTV may not be in an organized way, but in big cities of these continents, CCTV expansion is very rapid (Doyle, et. al., Eds. 2013). Likewise, in India, CCTV expansion is greatly enhancing but without any statue for protection of privacy (Singh, & Kumar, 2020). Such extension in CCTV systems also increases volume of database recorded through CCTVs, containing information pertaining to individuals. It requires some data protection regime.

CCTV Surveillance against Privacy and Data Protection

Personal Data Protection

Violation of Personal data is an infringement of personal privacy. Any sort of practice of selling of private information of any individual may amount to conceding to one's privacy (Sanjay & Menon, 2020). CCTV database misuses or abuses are no more a rare instance now days. These footages may go viral, either mistakenly or deliberately, by the data controller himself or by persons working under his control or by the persons working outside control in collision with the data controller and other persons in the organization having control of the CCTV footages. Such leakages of personal data may also amount to intrusion in privacy. To control such situations and such data breaches; data protection laws are of paramount consideration. Worldwide two models are available; First, American Model Fair Information Principles in nexus with OECD guidelines; secondly, EU data protection laws in the form of General Data Protection Regulations, 2018.

Fair Information Practice Principles (FIPPs) and OECD guidelines

Global increase in usage of CCTV may also have adverse impacts on data protection of individuals and privacy. Privacy once was completely sacrosanct. But buildup of personal databases may breach privacy of individuals. Alan worked on it in 1970s. In USA, it became a helping hand in formulation of "Fair Information Practice Principles" (FIPPs) which protects privacy rights as to personal data and envisages duties of the persons or organizations gathering data under Privacy Act, 1974. These regulations worked as a precursor for the laws of privacy worldwide. Such laws have further evolved. FIPPs still provide the core to all the available approaches (Wastin, 1967). There are the model guidelines influencing national or international laws on gathering data. These principles influenced the Organization of Economic Cooperation and Development (OECD) 1980 privacy guidelines (Wastin, 1967). The eight FIPPs principles under OECD guidelines are following;

(i) "Collection Limitation Principle": Collection of personal data should be subject to restrictions, gathered only through legal and fair ways, and with permission or knowledge of individual subjected to scrutiny.

(ii) "Data Quality Principle": Such data should be correct, all-inclusive, and updated one recorded for the purposes only.

(iii) "Purpose Specification Principle": The purposes of data collection should be provided before collection of it and any later usage of the data should only be limited to specified object.

(iv) "Use Limitation Principle": Any such data gathered ought not be made public or released. Usage has to be limited to stipulated purposes and not otherwise exception (a) with permission of the individual subject or (b) under the statute.

(v) "Security Safeguards Principle": Such data is sacrosanct, and protection should be provided with "reasonable security safeguards".

(vi) "Openness Principle": While personal data is gathered, its policy should be completely candor pertaining to guiding principles, practices, and their evolution. Availability of such data, its nature, usage according to object, and identification of "data controller" with his address should be ensured. It ensures transparency and honesty in collection of data; forbids secret data collection.

(vii) "Individual Participation Principle"

Data subject should be given right (a) to collect data from its controller or information as to availability data pertaining to him (b) to gain information as to data subject to charges which are not excessive. (c) to be provided with reasoning

for refusal of rights under above two clauses (a) & (b) while have remedy to challenge any refusal. (d) to confront any such decision of refusal, & in case he remains successful contesting such decision, such individual has a right to get removed, or modified or completed or corrected.

(viii) "**Accountability Principle":** Any violation of the above principles on the part of data controller should make him accountable for not complying with these principles (OCED, 1980).

Despite these principles and forth amendment in USA Constitution, USA follows the data market and surveillance approach under its PATROIT Act, it can have surveillance techniques in practice. Under the "principle of Third party", any data shared by the data subject or individual to the third party can be accessed by the law enforcement agencies in USA (Sharma, & Pranav, 2020).

That is why; FIPPS are criticized for not providing complete privacy and data protection. As the sole purpose of these FIPPs was not the privacy or personal data protection rather these were formed for better development, economical betterment, and surveillance. However, privacy and personal data protection have been the main concern of EU Data Protection Regulations, 2018.

At state levels, as to data recording, storing, and its protection, either done by public or private entities, it shall be regulated by the statutes of the state. States need to take effective steps so that the personal life or their data shall not be used or processed in any way by the individual against the object of ICCPR. Further, complete, and efficacious data protection should be provided to individual who should know about the authorities or persons collecting or controlling his data. In case, such data is in erroneous form, the data subject, the aggrieved person should be allowed to seek for its correction or deletion as per UN Human Rights Committee, General Comment No. 16, 1988. These principles are relevant to any personal data collected through CCTV systems as they envisage rights of data subject and imposes duties upon the controller of CCTV systems.

EU General Data Protection Regulation (GDPR), 2018

Prior to EU GDPR, 2018, the EU Data Protection Directives (DPD), 1995 were the main rules for data protection and free flow of the data in Europe. First, data subject ought to be given notice regarding gathering of the data. Secondly, collection of data should be purpose specific only. Thirdly, it is required to have consent of the data subject when his data is to be shared. Forth, no such gathered data should be misused or abused in any way. Fifthly, data controller is under duty to intimate data subject when his personal data is gathered. Sixthly, the individual should be given access to personal data and right of correction in case of any in-correction. Seventhly, on account of violation of any these above rules, data controller should be held accountable. This law was recently replaced with GDPR, 2018 which is applicable throughout the Europe and its application is extended to any of the Europeans regardless to the fact wherever they reside. The GDPR has the overriding effect on DPD and it is enforceable throughout the EU states since 2018. The key difference between both laws is that GDPR imposes more definite data safety obligations, and worldwide adaptability. Meanwhile, it imposes heavy penalties with strong execution process. It may result in strong personal data protection and less chances of its misuse. It imposes duties upon the data controller and its processors to safeguard sensitive data as well. Meanwhile, GDPR also envisage easy procedure for business (Lord, 2018).

These DPD seven principles are part of the GDPR, 2018. Under Article 5 GDPR envisages principles; "*Personal data shall be:*

> *(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')."*

It also envisages the principle of transparency; any CCTV system should not be installed in a secret or covert manner.

> *"(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation')."*
>
> *"(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data-minimization');"*

CCTV should only be installed for lawful purposes rather to harass or to intimate or to unlawfully intervention into the lives of other people around in the neighborhood or vicinity. If the purpose is specified for installation of CCTV, it must only be used solely for such an object. Meanwhile, Article 5 also mentions about the accuracy of data;

> *"(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');"*

It is the right of data subject and duty of data controller of CCTV to keep the stored footages or images in correct form and without any error in it. It is due to the fact any incorrect data may, at times, violate to the privacy rights of data subject and it may hurt to the person concerned.

It also requires that such data should also be removed or corrected if required by the concerned person. It basically ensures "right to be forgotten" under Article 17 of it. In addition, Article 15 of GDPR provides the data subject right to access the data recorded and to have the copy of it (Cusick, 2018). However, such data needs to be stored for the permitted period only. Article 15 also elaborates it;

> *"(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes….in order to safeguard the rights and freedoms of the data subject ('storage limitation');"*

It clearly means that CCTV data must be kept or stored within the time limit required for the purpose in case data subject, the person whose CCTV footage is recorded is identifiable. For Instance, purpose of CCTV may be the security of the public. Thus, data may be stored for such period. It is due to unnecessary and prolonged storing that may result into data abuse or misuse.

Another significant aspect of Article 15 and 13 to 22 is make duty bound to the data controller or possessor to ensure integrity and confidentiality of the data. In case, its integrity or confidentiality is breached, such person must be held responsible. Article 15 specially states;

> *"(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures ('integrity and confidentiality'). 2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')."*

It implies that CCTV footage must also be processed in such a way that no data leakage is possible while ensuring the safety of it from any illegal processing or its destruction. The chances of abuse or misuse of such data may enhance to optimum level when such data comes into the hands of persons who are not authorized to have access to it. It is pertinent to keep stored CCTV footage in confidential manner; thus, integrity of data and rights of data subject may be guarded. Meanwhile, strict, or rigorous accountability of the controller of CCTV of the data is indispensable.

Personal Data Processing and Balancing between Surveillance or Privacy

Personal Data is the information that can identify the individual and his identity. Any process that involves processing personal information falls under the domain of the GDPR. CCTV also processes the data. It collects data through cameras and stored in memory the processing of the data involves various steps; it may consist of the collection of data, recording, organization, security, alteration or deletion, dissemination and other steps (Sharma & Pranv, 2020). Regarding processing of personal information, Article 4(1) of GDPR states; *"The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data."* These steps also involve in CCTV surveillance regardless to the fact such surveillance system is operated either by oneself or some 3rd party in one's behalf. Such person would be data controller who processed the data. Any breach of such data may amount to infringement into privacy and personal data protection. The *supra* seven data protection principles would come into play if any breach or abuse of data occurs.

However, there is need to balance between the data protection, surveillance and privacy on realistic approach as the states and their ground realities are not universal despite human rights activist's approach leaning towards the universalism of human rights. States globally practice CCTV surveillance including states like USA, UK after 9/11, or many states including Pakistan or India, subject to certain EU states i.e., Norway, Germany or outside EU Canada.

Such equilibrium is possible through at least three measures when processing personal data involves privacy; legality of processing data, necessity and proportionality. These measures detailed by EU Court, and GDPR have provided the balancing act; if the states adopt it legality purpose is completed. Necessity or proportionality depends are the

questions of fact and may vary case to case. EU GDPR includes these principles and it incorporates when these regulations may not be applicable. For balancing between CCTV surveillance, privacy and data protection further following three points of GDPR are of paramount consideration;

Non-Application of GDPR

Like every good law, GDPR also has certain exceptions wherein these rules do not apply in terms of its Article 2(2), 23 and 49. First, these rules do not apply outside European Countries or on Non-EU states' citizens. Secondly, these rules are not applicable in case authorities are processing data for prohibition of crimes during investigation, detection, or prosecution, for public security or maintenance of peace or tranquility in the society, enforcement of orders of courts as to guilty of the convicts or civil obedience, security of state and other likewise activities.

In this way, it may be said that CCTV installed for the above-mentioned purposes has been given protection of law. However, other rights of the data subject cannot be subject to violations. Rather those rights are protected to ensure privacy and individual freedom. It may not be wrong to aver that usage of CCTV and its data must proportionate the need for these purposes. Any extensive usage such technology is still forbidden against the rights of data subject.

Independent authority to monitor enforcement of regulations

Chapter 6 of GDPR 2018 is significant for data protection as it requires EU states to establish some authority or commission on privacy and data protection which shall be independent and efficient in its working. It must not be in any way subject to undue influence of the government concerned. Among other tasks of the authority, the main significant portion is that a data subject can complain to such an authority which shall be having mandate to independently investigate into the allegations of data breaches or misuses.

Penalty on violation of regulations

Regulations requires data controller to report any data breach in case such violation amounts to threat to the rights and liberties of the data subject within the span of seventy-two hours. In case of non-compliance, huge amount to the extent of 20 million euros or more may be imposed. Meanwhile, organizations and institution must make sure that they are following these regulations in the letter and spirit.

It implies that CCTV surveillance shall be subject to legality, necessity and proportionality principles in nexus with the data subject rights available in GDPR, 2018. Any violation shall be investigated and tried by the independent authority which shall penalize the data breaches adversely affecting privacy. However, in *supra* mentioned exceptional situations, even under GDPR, states can use CCTV surveillance. Implementing these three points in conjunction may bring positive fruits for the data subject rights, state's concerns for protection and security or data processor.

Conclusion

Generally, privacy and data protection are sacrosanct, but it is not a right available in all the situations. Excessive usage of CCTV system may adversely affect the personal freedoms of the individuals. Almost all over the world, such technology usage has been enhancing day by day. There is no doubt about the fact that individuals have privacy in their personal premises i.e., their homes and such private places.

However, privacy in public spaces is subject to varied opinions; it maybe not wrong to say that there is difference of opinion on the issue. The USA Supreme Court in *supra United States v. Hester*, and *Oliver v. United States*, cases, decided that privacy is limited to *"houses, persons or their letters or their affects"* only. It is not extended to open field. It is evident from increase of CCTVs surveillance in USA. The impetus to which can be found after 9/11 not only in USA, but also worldwide. Still, data recorded by CCTVs are still subject to FIPP in USA.

In contrast, EU has different, but better standards for protection of privacy of its citizens. In *supra Peck* case, EU Court of HR held that CCTV surveillance can be allowed in public places and individual freedoms or privacy is not affected by such system unless and until CCTV records data of the data subject. This is certainly a different position of EU from that of US Supreme Court's *"open field doctrine"*. It means individual right of privacy has certain protections even in public spaces. Meanwhile, EU model of data protection regulations are more extensively covering protection of individual personal data protection. GDPR 2018 applies to CCTV systems. Any data recorded through CCTV comes under the domain of these regulations; all the rights of data subjects and duties on data controller provided in GDPR apply during CCTV surveillance. Though, these regulations even provide certain exceptions of national security, detection or prosecution of criminals and others. Same is the opinion of Human Right Committee envisaged in its General Comment No. 16. It generally prohibits all type surveillances including CCTV, but the privacy is subject to public interest.

However, it is in no way meant that state or its authorities or individuals or private organizations are free to operate CCTV systems as they like. CCTV surveillance must not exceed the limits of doctrine of legality, proportionality or necessity. It means there must be some law that regulates such technology. No one should be allowed to use CCTVs against the laws. Meanwhile, such law also provides the necessity test that would check whether CCTVs installation is required or not. If it is required, it must pass out the proportionality test that would see whether the amount of breach to right of privacy is excessive or not than the purpose for which CCTV was installed. If the answer is affirmative, CCTV usage maybe allowed, subject to regulations. In case, the answer is contrary, usage of CCTV should not be allowed.

References:

ALibeigi, A., Munir, A. B., & Karim, M. (2019). Right to Privacy, a Complicated Concept to Review. *Right to Privacy, A Complicated Concept to Review*.

Agustina, J. R., & Clavell, G. G. (2011). The impact of CCTV on fundamental rights and crime prevention strategies: The case of the Catalan Control Commission of Video surveillance Devices. *Computer law & security review*, *27*(2), 168-174.

Ball, K., Haggerty, K., & Lyon, D. (2012). *Routledge handbook of surveillance studies*. Routledge. (London and New York: Taylor & Francis, 2012): 225.

Banisar, D., & Davies, S. (1999). Privacy and human rights: An international survey of privacy laws and practice. *Global Internet Liberty Campaign*. Available at https://www.researchgate.net/publication/242448871_Privacy_human_rightsan_international_survey_of_privacy_laws_and_developments

Barrett, D. (2013). One surveillance camera for every 11 people in Britain, says CCTV survey. *The Telegraph*, *10*. Available at http://w3.salemstate.edu/~pglasser/One_surveillance_camera_for_every_11_people_in_Britain__says_CCTV_survey_-_Telegraph.pdf

Brandeis, L., & Warren, S. (1890). The right to privacy. *Harvard law review*, *4*(5), 193-220. Also available at https://www.stetson.edu/law/studyabroad/spain/media/Wk3.Stuart.Day1-1-THE-RIGHT-TO-PRIVACY-(excerpt).pdf

Cheung, A. S. (2014). Revisiting privacy and dignity: online shaming in the global e-village. *Laws*, *3*(2), 301-326.available at https://doi.org/10.3390/laws3020301 accessed on 21-12-2020.

Clearinghouse, P. R. (2004). A review of the fair information principles: The foundation of privacy public policy. *Retrieved September 1*, 2005.

Cusick, J. (2018). The General Data Protection Regulation (GDPR): What Organizations Need to Know. *CT corporation resource center*, 1-6.

Diggelmann, O., & Cleis, M. N. (2014). How the right to privacy became a Human Right. *Human Rights Law Review*, *14*(3), 441-458.

Doyle, A., Lippert, R., & Lyon, D. (Eds.). (2013). *Eyes everywhere: The global growth of camera surveillance*. Routledge.

Edwards, L. (2005). Switching off the surveillance society? Legal regulation of CCTV in the UK. Asser Press.

European Union Data Protection Directives. (1995).

Floridi, L. (2016). On human dignity as a foundation for the right to privacy. *Philosophy &*

Technology, *29*(4), 307-312.

Fair Information Practices Principles.

Gassmann, H. P. (1981). OECD guidelines governing the protection of privacy and transborder flows of personal data. *Computer Networks (1976)*, *5*(2), 127-141. Also available at https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf (accessed on 03-02-2020)

General Data Protection Regulations. (2018).

Ghani, A. (2019). Not investigating CCTV footage leak from Lahore's cinema: FIA Cyber Crime Wing. *Digital Rights Monitor*. Retrieved from https://www.digitalrightsmonitor.pk/not-investigating-cctv-footage-leak-from-lahores-cinema-dg-fia-cyber-crime-wing/

Gross, E. (2004). The struggle of a democracy against terrorism-protection of human rights: the right to privacy versus the national interest-the proper balance. *Cornell Int'l LJ*, *37*, 27.

Hempel, L., & Eric, T. (n.d.). Urban Eye: Final Report to the European Commission. 5th Framework Programme, Working paper No. 15. Berlin. *Technical University of Berlin*. Retrieved from https://d1wqtxts1xzle7.cloudfront.net/33484200/routledge_handbook_of_surveillance_studies.pdf?1397655880=&response-content-disposition=inline%3B+filename%3DRoutledge_Handbook_of_Surveillance_Studi.pdf&Expires=1610790843&Signature=RUKWUcPtsocHYvAkTw6wDADS5Jo8bytk1EsQNQ2Uh99cM4tQf4ODM3zvSiQK8eTQnp8tiGH7aaXKjpRu1zGo0Gv2gRaov83MBDNEg86aSE4dGQgUwh2Wz3f6hnHCP6AbnoDOn98SQwxZZqT3hOwYcrGaVpSH7QJwprGX7oSbR96VJQo~FpiMOv5HkSm0HIt6fiUozOVgv6WPu-XhxaspaR0L84AbzaoAbgtoXuI3Y9bAuiy-3ki2q3iFqRlftE3eZqEVOwZRoHRLkMTWm37mqdYY~z8rd~-G8a9yBvrpPruppIIFcXKoQLAaeQc-X86rQ9bXvkr-R-G30B9IBsfxTg__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA#page=258

Holvast, J. (2009). History of Privacy. *Conference: IFIP Summer School on the Future of Identity in the Information Society.* Retrieved from https://www.researchgate.net/publication/225802214_History_of_Privacy accessed 22-12-2020

International Covenant on Civil and Political Rights. (1966).

Katz v. United State. (1967). 389 US: 347

Lord, N. (2018). What is the Data Protection Directive? The Predecessor to the GDPR. DIGITALGUARDIAN.

Lyon, D. (2007). Surveillance studies: An overview.

Lukács, A. (2016). What is privacy? The history and definition of privacy.,

Noris, C. (2012). Accounting for the global growth of CCTV. *Routledge Handbook of Surveillance Studies, ed.* Kirstie Ball, Kevin D. Haggerty & David Lyon. (London and New York: Taylor & Francis: 251.

Oliver v. United States. (1984). 466 U.S:170.

Owsley, B. L. (2014). TriggerFish, StingRays, and Fourth Amendment Fishing Expeditions. *Hastings LJ*, *66*, 183.

Peck v. United Kingdom. (2003). 36 E.H.R.R: 41.

Perry-Hazan, L., & Birnhack, M. (2019). Caught on camera: Teachers' surveillance in schools. *Teaching and teacher education*, *78*, 193-204.

Paterson, M. (2009). Surveillance in Public Places and the Role of the Media: Achieving an

Optimal Balance. *Media and Arts Law Review*, *14*(3), 241.

Richards, N. M. (1934). The Dangers of Surveillance, 126 Harv. *L. Rev*, *1965*, 2013.

Scott v. Harris. (2007). 05-1631. U.S.: 550.

Gutwirth, S., Leenes, R., Hert, L.P.D., Poullet, Y. (2013). European Data Protection: Coming of Age Chapter: Seven Types of Privacy. *Springer.*

Sharma, S., & Pranav, M. (2020). Data Privacy and GDPR Handbook. *John Wiley & Sons, Inc., Hoboken, New Jersey*. P:38.

Singh, P., & Kumar, G. (2020). Why Am I Under CCTV Surveillance? Available at https://jilsblognujs.wordpress.com/2020/05/16/why-am-i-under-cctv-surveillance/

Tridimas, T. (1999). *The general principles of EC law*. Oxford University Press, USA.

Universal declaration of human rights. (1948). *UN General Assembly*, *302*(2), 14-25. http://www.verklaringwarenatuur.org/Downloads_files/Universal%20Declaration%20of%20Human%20Rights.pdf

United States v. Hester. (1924). 265 U.S.: 57.

UN Human Rights Committee. (1998). CCPR Gen. Comment # 16, Art. 17 The right of privacy, family, home and correspondence and protection of Honour and Reputation. Available at https://www.refworld.org/docid/453883f922.html

US Department of Homeland Security. (2013). CCTV Technology Handbook. available at https://www.dhs.gov/sites/default/files/publications/CCTV-Tech-HBK_0713-508.pdf (last assessed on 20-09-2020)

Vermeulen, M., & Bellanova, R. (2012). European Smart Surveillance: What's at Stake for Data Protection, Privacy and Non-Discrimination. *Sec. & Hum. Rts.*, *23*, 297.

Westin, A. F. (1968). Privacy and freedom. *Washington and Lee Law Review*, *25*(1), 166.

Wood, D. M., Ball, K., Lyon, D., Norris, C., & Raab, C. (2006). A report on the surveillance society. *Surveillance Studies Network, UK*.