Journal of Contemporary Issues in Business and Government Vol. 27, No. 1, 2021
P-ISSN: 2204-1990; E-ISSN: 1323-6903
https://cibg.org.au/

Entity Of Privacy In The Era Of Technology

PRITHIVI RAJ[1], MURTAZA S. NOORANI[2]

[1]*Assistant Professor of Law, ICFAI University, Himachal Pradesh, India*
[2]*Student, A.K.K. New Law Academy, Pune, India*

ABSTRACT

The shifting sense of privacy from one social background to the next, notably in the eyes of the law, has been a persistent challenge. Technology when seen from the lens of privacy in educational institutions poses a significant threat to the safety and security of all, the most vulnerable and exposed being- young girls, female teachers with the threat of stalking and voyeurism. Furthermore, it is a flagrant breach of students' and teachers' right to privacy and freedom of speech and expression. Notably, there are no regulations or legislation in place to control the installation of surveillance and data collection devices like CCTV or other monitoring/ data collection equipment in Educational Institutes for the purposes of safety, security and regulation. The authors would also examine the above in terms of the right to privacy, necessity and legality. The authors will attempt to showcase reality on the ground along with legal landmarks to satisfy the object and rationale behind the research.

KEYWORDS: Right to Privacy, Technology and Privacy.

1. INTRODUCTION

In modern culture, privacy has come to be synonymous with things like "freedom of speech, sovereignty over one's body, isolation in one's home, autonomy over personal knowledge, freedom from observation, security of one's identity, and protection from searches and interrogations," among other things. Since then, the constant challenge has been to find these principles of choice, explain the shift from one social context to another, and find a legal basis for personal control. This article is looking for answers to the structural changes and legal perceptions of modern social communication. In Peck (2003), the European Court of Justice decided to protect his privacy from freedom of expression when footage of Peck's suicide attempt was broadcast by CCTV cameras without properly hiding his identity on public roads. The court ruled that the applicant was "on public streets... but he was not here to participate in public events, and that it was not public extradition." Public protests against his image "far exceeded the impact on the adversary or guards. ... [he] could possibly have predicted it." Therefore, without his consent, the media should not disclose their identities for legitimate purposes of reporting the effectiveness of video surveillance systems in crime prevention. Confidentiality was also guaranteed on the day when unauthorized photos of the royal family were posted in Monaco in Von Hannover (2004). "The court was in session. The

public had no legitimate interest in knowing where the applicant is and how she generally behaves personally, as the case caught had nothing to do with her public activity. Well known to the public it is called remote.
In White (2006), freedom of speech became evident, but it was announced with the release of "balanced" and "real" accounts of Palme's murder tort. This time, because the applicant was already well-known and the issue was of serious public interest and concern, the court decided that "there is less scope to limit the transfer of information."
In each of the last three cases, "the decisive factor in balancing integrity and freedom of expression" was the public's contribution to the "common interest debate" in a democratic society. Here, the courts have made an important distinction between the two functions of the media.
a) "watch dog" of a democratic society f
b) A source of "entertainment" or "curiosity" for a "specific reader".

Confidentiality case law is still in its infancy. However, the axis of gravity can appear in the judiciary. In other words, when the same case is tried in the same way, it can manifest itself in at least some top appeals. Functional relevance appears to be a universal but tacit standard that appears in legal reports of various confidentiality conflicts. Of course, the best protection of privacy or consistent informed judgment cannot definitively set the boundaries of social systems. Structural changes in social communication are constantly changing the boundaries of the system and creating new contradictions between them. A new confidentiality conflict occurs. The line between legal and illegal is blurred. And again, the court is required by law to determine public and private. Thus, new confidentiality rights emerged in the last century, with new "trends" for private realms that were previously considered. Until the 1970s, violence against women was protected, for example, by the laws of family integrity and family harmony (Siegel, 1996). Today, however, confidentiality is recognized in close relations in many Western countries, with the potential for sexual assault, domestic violence and child abuse. While privacy has gone beyond white, upper-class heterosexual men in making certain physical and mental decisions, the elites appear to have lost their previous control over the transfer of personal information to the media. Legal differences between many media functions and differences between important and unrelated functional aspects of public life can partially restore these controls. Finally, like any other law, legal privacy can constitute expectations. They can't decide what to do. The increasing number of confidentiality disputes and the intermittent nature of legal responses to them shows the extent to which such expectations cannot be sustained. But confidence in the potential for cure actually absorbs most of the risk of confidentiality breaches. As long as the general expectation of confidentiality is maintained, a breach of confidentiality or a large breach may be tolerated in court decisions. This can explain the widespread exaggeration of the unintended consequences of cyberspace and surveillance transactions and the increased sensitivity to privacy.

2. CASES OF SURVEILLANCE DUE TO ENHANCEMENT IN TECHNOLOGY AND ITS EFFECT.

During national crises, citizens are often encouraged to sacrifice freedom and integrity for safety. And if we can get enough security with a little integrity, why not? Security surveillance shouldn't be too annoying or life-changing. This does not mean that authorities have to physically search every suspect or person associated with the suspect. Advances in digital technology have made these observations relatively inconspicuous. Video surveillance, global positioning systems, airport scanners and biometrics technologies provide law enforcement surveillance tools without the burden of surveillance targets along with data surveillance. This view is contrary to those who argue that we should be concerned about the integrity of the trade for safety. It is said that criminals and terrorists are not as dangerous as the government. We have too many examples to deny Sir Acton's statement that "power tends to corrupt and absolute power tends to corrupt absolutely." If control over your information gives you full awareness and power over the information, then there are good reasons to stop trading secrets for security reasons. Power is the ability to force demand access to information about others while keeping your own information confidential. Governments and businesses are known to be good at demanding access to information. The latest response to this trend has been the emergence of online information-sharing websites that highlight the activities of authorities and businesses behind the scenes. Web sites like WikiLeaks are committed to changing the environment of responsibility. Previously, it was argued that individuals enjoyed moral protections that limit state surveillance practices. While your right to privacy is not absolute, it protects people from the eyes and ears of neighbors, businesses and countries. The problem we are seeing in this article is balance. When are sufficient security interests important to compensate for an individual's privacy rights?

If the state is placed as a central concept, cyber security and cyber monitoring are two sides of the same coin. In a sense, the subjects are tied to the state in terms of protection and welfare. The real risk the subjects face as a result of being monitored is none other than the State. The author argues from the perspective of a technology user's concern for privacy, which is logically demanded from another user, the state, and the corporate- also forming a golden triangle.

The respect for privacy between one consumer and another is often driven by monetary and criminal issues. Although the relationship between a user of a technology and the service provider is usually regulated and established by policies and agreements, However, as seen from the author's perspective, the interaction between a consumer of technology and the state in contemporary parlance is far larger than the one between individuals or companies. Since the role of the state is not limited to security and governance as in a conventional democratic structure. It had become even larger, with arguably unchecked forces. The state serves as a defender, distributor, and enforcer.

Now, why do people, as subjects of the State, and Corporations, who are bound by the framework and policies of the State, have an ever-increasing concern about their privacy

when it falls into the hands of the state? To put it simply, it is for the obvious purpose that it may be used against them or to stifle their opinions, expressions, and convictions if they do not meet the state's expectations.

We question the prehistoric pluralism and existing legal definitions of national security, friendly relations with foreign countries, public order, dignity or morality or blasphemy, slander or incitement to crime, despite valuable research on secrecy must be raised from a socio-psychological, systematic, network perspective.

One way to strike a balance between privacy and security is to let those in power decide. In most cases, these individuals seek public office for noble purposes—we should let them decide how best to protect privacy and security. This position is called "just trust us." The second comment alleviates privacy concerns by questioning the steps that confidentiality can cover up. This view of "nothing to hide" argues that people shouldn't worry about being watched. Only those who engage in immoral and illegal activities should worry about government surveillance. It looks like "nothing to hide"-this is the "most important" view. The latest version claims that the security interests are inherently more convincing than asking for privacy. By criticizing these balanced efforts, we will defend our own case by drawing conclusions, giving an arbitrary legal position when making orders, showing possible causes of interference, and allowing the public to review the proceedings. Will, and you can promote both through proper logic. Integrity and security. Finally, in the final section, we look at the technology mobility and development and its impact on privacy.

"JUST TRUST US"—TRADING CIVIL RIGHTS FOR SECURITY"

Prior to actually delving into the "just trust us" viewpoint, we would want to briefly discuss why we should regard privacy and security as morally important. Privacy, described as the right to regulate access to and use of one's own body, place, and knowledge, is essential for human well-being or flourishing. Simply put, there is ample evidence that people who lack this kind of regulation fail physically and psychologically. Safety is also important. The legal function of all governments is to protect the rights of the people, whether it comes from the individual's right to self-defense or the right to social consensus. At the most basic level, security gives people control over their lives, projects, and property. To be safe at this level, you must have sovereignty over your private domain. There should be no unnecessary interference from others, companies and governments. Security also protects groups, companies and businesses from excessive disruption to projects and assets. Without such controls, businesses and businesses could not operate in the free market for at least for a long time. National security must also be considered. Here we are concerned about the continued existence of political alliances. Our institutions and markets must be protected from foreign invasion, epidemics and terrorism. But we take national security seriously, not because a particular political alliance is valuable in itself, but because it is an essential part of protecting individual rights.

3. NEED FOR A SOUND POLICY FOR PROTECTION PRIVACY IN THE ERA OF TECHNOLOGY

There is a fine line that divides and interferes with the moral right to privacy and moral liberty. Privacy is a right *in rem* right, meaning it extends to the whole world. The right to be left alone. However, in this day and age, where the meaning of public and private spaces is shifting, the principle of privacy is also experiencing a complex change. To elaborate, consider the following two contrasts: Previously, a person's physical distance from the community would be sufficient to protect his right to privacy. Whereas this is not always the case in modern times, the individual may be alone while being watched and followed.

An open society is not inevitable. Personal integrity can be achieved through personal and social pressure. Confidentiality associated with the media, corporate and government's primary interests can be guaranteed by law and is socially modified and based. Judge Douglas said Osborne v. America: "There may be times when no one can be sure that his words will be recorded for future use. When everyone is afraid that they are no longer in their own inner thoughts, but in the government; When the most secret and intimate conversations are always open to the ears of curious impatience. When that time comes, loneliness and freedom will disappear. Who can say it's free if the privacy of the chosen person could be violated who can say that he exercises freedom of speech if all his words are written and judged, or if there is a fear that all words can speak? If all communication is known and recorded, and conversations with colleagues are stolen, who can say that he is free to socialize? When such a situation arises, our citizens will be afraid to express thoughts other than the safest and most orthodox ones. Fear of communicating with someone other than the most acceptable person. The freedom provided to the constitution will be lost. Douglas paints a serious picture. We must heed his warnings. We have good reason to resist our journey to an observer-based society. Transparency is not required for security. Finding the right balance between privacy and security is difficult. However, it is argued that these two important values are best defended by pursuing possible causes, judicial discretion, and public investigation. Serious violations of fundamental rights due to influence on the supervision and other basic rights of the state, other institutions and actors.

SURVEILLANCE AND RIGHT TO LIFE AND PERSONAL LIBERTY

The design of Bentham Panopticon Prison made it appropriate to make an analogy with Foucault's social analysis. Foucault said the architectural project symbolizes how Panoptical was empowered while inmates were exposed to "objects of knowledge, not objects of communication." The panoptic model was used to show how uncertainty can be used as a means of social control. Bentham's model represents the idea of a ubiquitous gaze, which is why powerful technology leads to surveillance. The mystery and doubt about whether or not the infant is being watched contributes to the panoptic influence of surveillance device, which has the effect of self-policing. In K.*S Puttaswamy* the need to protect individuals from such scrutiny, by citing *Gobind v. State of M.P* wherein it said, "Individuals need a sanctuary where they can be free from societal control. The importance of such a sanctuary is that individuals can drop the mask, desist for a while from projecting on the world the image they

want to be accepted as themselves, an image that may reflect the values of their peers rather than the realities of their natures." A educational shelter is one that needs certain safeguards. It is important for a learning environment for students not to be burdened by parental anxiety and demands. At, Puttaswamy helps carve out a collective right of children to study in private, where the panoptic state does not lead them to self-police their conduct, stating, "The disconcerting effect of watching another look over one's shoulder while reading or writing explains why individuals would prefer to retain their privacy even in public."

ADVERSE IMPACT OF VIOLATION OF PRIVACY ON FEMALES

The right to privacy entails not only the right to prohibit the inaccurate portrayal of private life, but also the right to prevent it from being portrayed at all. There are already significant differences, and women's realities are increasingly shifting, with new forms of discrimination against them emerging regularly. Some women face additional types of prejudice on the basis of their age, race, nationality, religion, health status, marital status, occupation, disability, and socioeconomic status, among other factors. When designing policies and proposals to address sexism against women, these interweaving types of discrimination must be considered.

Continuous surveillance and monitoring opens people to the eyes of others they do not want to be watched or tracked by. It is particularly harmful to young girls and does significant harm to them. Such intrusive society, for example, will violate women's privacy during their menstrual periods. Women of a younger age may be unsure of how to care about their sexual health. It is natural to be perplexed by the sudden changes that the body goes through, especially given the unique social stresses that women face. Concerns about menstrual health and sanitation are particularly important in how women treat themselves during their cycle. It is unreasonable to expose such private acts to public inspection, and it amounts to a blatant breach of the children's and female teachers' rights to dignity. It is also unclear what procedures are in place to protect the information collected from abuse by schools, governments, or third parties with access. Reading the 2018 Personal Data Act, which includes personal data, shows that the state can collect and process large amounts of student and teacher data and personal data in the classroom. In the absence of effective judicial plans, legislation and mechanisms, the controversial policy would violate Puttaswamy, as courts admit that modern technology must permanently store information about a person and his actions. "Privacy of children will require special protection not in context of the virtual world, but also the real world."

THE JUSTICE B.N. SRIKRISHNA EXPERT COMMITTEE REPORT:

According to reports on the protection of children's personal data, children's personal data should be protected more than with conventional data processing. The report of the expert committee explicitly contains the legal obligations of all trustees to process data on children. The same requirements are also contained in Article 23 of the Privacy Act. According to Article 16 of the 1989 Convention on the Rights of the Child, signed by India, "A child must not receive arbitrary or illegal interference with or illegally infringe on his or her privacy, home or correspondence. The second paragraph of the complaint also states that children

have the right to be protected by law from such harassment or abuse. Are more susceptible to exploitation by Internet users. The government has not proposed a solution to these data protection problems. Wrong hands can have serious consequences.

4. IMPACT OF TECHNOLOGY ON RIGHT TO FREEDOM OF SPEECH AND EXPRESSION

Hon'ble Supreme Court in the case of *Ministry of Information & Broadcasting, Govt. of India v. Cricket Association of Bengal*, held that the right to free speech and expression requires the rights to educate, inform, and entertain, as well as the right to be taught, informed, and entertained. This was upheld by a constitution bench in *State of Karnataka v. Associated Management of English Medium Primary & Secondary Schools*. Further, Puttaswamy states "Privacy in all its aspects constitutes the springboard for the exercise of the freedoms guaranteed by Article 19(1). Freedom of speech and expression is always dependent on the capacity to think, read and write in private and is often exercised in a state of privacy, to the exclusion of those not intended to be spoken to or communicated with." The innate right to speak and express oneself is profoundly rooted in the practise of learning. Exercising verbal independence necessitates cognitive freedom. Classrooms should be places where children can freely express their desires, ideologies, and opinions without fear of being constantly watched.

As held in *PUCL v. Union of India*, held that Freedom of expression, which overlaps with freedom of speech, is not limited to verbal or written expression; it also involves the expression of any emotion. Visual tracking, as defined in Article 19(1), allows one to track speech and expression (a). For instance, if parents want their children to speak up in class, children who do not do so will be pressured to speak up. The devices will document the teachers' instructional materials on show, such as blackboard notes or PowerPoint presentations. Here are some explanations to demonstrate this: A lesson on sex education is presented to students, and there is a map on the board that clearly illustrates what the subject of conversation in class is; students are unable to ask questions because they are afraid of being watched, which stifles their voice. There is a high degree of awareness needed for students to be familiar with reproductive health concerns. Conversations and interviews on these topics have a profound effect on the development of adolescent brains. Regrettably, our culture has a strong aversion to addressing these issues. It is critical that such discussions take place publicly among students and teachers without fear of being witnessed by the wider community. The idea that one is being followed will amplify the negativity associated with this and ultimately jeopardize the likelihood of truthful **a**nd inquisitive discussions. When coping with politically or historically controversial subjects, an instructor can attempt to discourage class debate in order to avoid being accused of inciting students' emotions or "propagandizing" them**.** In the case of *Kharak Singh v. State of U.P.*, the constitution bench held that merely executive or departmental instructions would not be "a law" that the state is entitled to make under the relevant clauses (2) to (6) of Article 19 in order to regulate or curtail fundamental rights guaranteed by the Article 19(1). Also In the case of *Bijoe Emmanuel and Ors. v. State of Kerala and Ors.*, the Court upheld this.

5. CONCLUSION

In this article, we have argued that balancing tests designed to illustrate privacy invasions in the interest of security often fail and attempt to exchange values that are difficult to quantify. It has also been suggested that we should rely on probable cause, judicial oversight, and accountability in exchange for privacy. Probable cause provides the standard for deciding whether security interests triumph privacy rights. Judicial review brings an "objective" investigator into the mechanism by being open to case-specific information such as the context and severity of the potential intervention. Sunlight laws permit a public debate on the legality of individual searches and seizures. All of this encourages transparency by making the rationale for a search and the conduct of elected officers known. Another advantage of such policies is that they foster loyalty and faith in elected leaders. An open culture should not have to be unachievable. Personal privacy can be protected by tradition and social pressure. Privacy in regards to the media, corporate interests, and the State can indeed be covered by statute as well as by traditions and social activities. There are many forms of privacy-privacy tradeoffs. They can be unexpected and undesirable at times The incidences of breach and violation that occur on a daily basis are self-speaking that there is a huge gap in our policies and something's are fundamentally wrong in our system which need to be urgently be looked into and fixed, since it is more a matter of justice than mere right. Freedom as the Constitution envisages will be vanished. Significant intellectual interest in the right to privacy seems to be centered on describing the definition of privacy The prudent way to protect this important values is to insist on a probable cause requirement, judicial discretion, and public oversight, which in the authors view can only be achieved by a sound policy and an active and independent judiciary.

6. REFERENCES

[1] Shiv Shankar Singh, Privacy And Data Protection In India: A Critical Assessment, Journal Of The Indian Law Institute , October-December 2011, Vol. 53, No. 4 Pp. 663-677 Published By: Indian Law Institute.

[2] David E. Pozen, Privacy-Privacy Trade Offs The University Of Chicago Law Review Vol. 83, No. 1 (Winter 2016), Pp. 221-247 (27 Pages) Published By: University Of Chicago

[3] .J. Angelo Cor, The Nature And Value Of The Moral Right To Privacy, Public Affairs Quarterly Volume 16, Number 4, October 2002

[4] Katayoun Baghai, Privacy As A Human Right: Sociological Theory Author, Sociology, Vol. 46, No. 5, Special Issue: The Sociology Of Human Rights (October 2012), Pp. 951-965 Published By: Sage Publications, Ltd.

[5] Lord Acton, Letter To Bishop Mandell Creighton (April 3, 1887), In The Life And Letters Of Mandell Creighton, Ed. Louise Creighton (New York: Longmans, Green, 1904), Vol. L,Chap. 13

[6] Adam D. Moore, Privacy Rights: Moral And Legal Foundations (University Park, Pa: Penn State University Press, 2010).

[7] Adam D. Moore, Privacy, Security, And Government Surveillance: Wikileaks And The New Accountability, Public Affairs Quarterly, Vol. 25, No. 2 (April 2011), Pp. 141-156 Published By: University Of Illinois Press On Behalf Of North American Philosophical Publications
[8] Supreme Court Of The United States, 530 U.S. 1237; 120 S. Ct. 2676; 147 L. Ed. 2d 287; 2000 U.S. Lexis 4126; 68 U.S.L.W. 3756, June 12, 2000, Pp. 341-35
[9] Daniel J. Solove, Understanding Privacy, The University Of Chicago Law Review Vol. 83, No. 1 (Winter 2016), Pp. 221-247 (27 Pages) Published By: University Of Chicago
[10] Peck V. The United Kingdom, No. 44647/98, 62, Echr 2003.
[11] Von Hannover V. Germany, No. 59320/00, 77, Echr 2004.
[12] White V. Sweden, No. 42435/02, 29, Echr 2006.
[13] Kantaru Rajeevaru V. Indian Young Lawyers Association And Ors. Review Petition (Civil) No. 3358/2018 (Sabrimala Review Judgement)
[14] K.S Puttaswamy v. Union of India, (2017) 10 SCC 1
[15] Gobind v. State of M.P, (1975) 2 SCC 148
[16] Ministry of Information & Broadcasting, Govt. of India v. Cricket Association of Bengal, 1995 SCC (2) 161
[17] State of Karnataka v. Associated Management of English Medium Primary & Secondary Schools, (1994) 1 SCC 550]
[18] PUCL v. Union of India, AIR 1997 SC 568
[19] Kharak Singh v. State of U.P, 1964 SCR (1) 332
[20] Bijoe Emmanuel and Ors. v. State of Kerala and Ors, 1986 SCC (3) 615