UGC & Govt. Approved
Sonargaon University (SU)
সোনারগাঁও ইউনিভার্সিটি (এসইউ)

Research Monograph

On

"A Comparative Analysis of National Security Legislation and the Right to Privacy in the Digital Era: Lessons from the U.S., U.K., and India"

Research Paper submitted in partial fulfillment of the requirements of the Bachelor of Laws with Honor's (LL.B) under Sonargaon University

Submitted To:

Sunzida Akhter

Lecturer

Department of Law

Sonargaon University

Submitted By

MD Naim Uddin

ID No: LLB 2102023025

Batch-23rd

Department of Law

Sonargaon University

Date of Submission: 08 July, 2025

LETTER OF TRANSMITTAL

Date : 08 July, 2025

To
Sunzida Akhter
Lecturer
Department of Law
Sonargaon University

Subject : Letter regarding the Submission of Research Monograph on "A Comparative Analysis of National Security Legislation and the Right to Privacy in the Digital Era: Lessons from the U.S., U.K., and India"

Dear Madam,
I an hereby pleased to submit the project on "A Comparative Analysis of National Security Legislation and the Right to Privacy in the Digital Era: Lessons from the U.S., U.K., and India". It was a great pleasure to work on such an important topic. This project was assigned to me in partial fulfillment of the requirements for the award of the degree Bachelor of Laws from Sonargaon University.

I believe that this project will certainly help you in evaluating my work. I would be very happy to provide any assistance in interpreting any part of the paper whenever necessary.

Sincerely yours,

……
MD Naim Uddin
ID No: LLB 2102023025
Batch-23rd
Department of Law
Sonargaon University

STUDENT DECLARATION

I hereby do solemnly declare that the work presented in this dissertation paper has been carried out by me and has not been previously submitted to any other University/College/institution/Organization for academic qualification or professional degree.

I hereby assure that the work that has been presented here does not breach any existing copyright law.

I further undertake to indemnify the University against any loss or damage arising from breach of the forgoing obligations.

Signature

.....

MD Naim Uddin
ID No: LLB 2102023025
Batch-23rd
Department of Law
Sonargaon University

CERTIFICATION

This is to certify that the Research Monograph on **"A Comparative Analysis of National Security Legislation and the Right to Privacy in the Digital Era: Lessons from the U.S., U.K., and India"** is the bonafide record of the project work done by MD Naim Uddin, ID No: LLB 2102023025 in partial fulfillment of the requirements for the award of the degree of the Bachelor of Laws, Sonargaon University.

I do here by certify that the project work has been carried out under my direct supervision and guidance.

……

Sunzida Akhter
Lecturer
Department of Law
Sonargaon University

ACKHOWLEDGEMENT

At first, I would like to thank Almighty Allah for his kindness on me in accomplishing the report. I would like to express my deep sense of gratitude to my honorable and distinguished supervisor **Sunzida Akhter,** Lecturer, Department of Law, Sonargaon University for her individual suggestions, valuable time, important information and guidance during the study period that has greatly inspired me in preparing this report successfully.

It could not possible to think all those people who have contributed for the preparation of this Research. Of course there are some very special names that cannot be forgotten. I am also grateful to the Department of Law, Sonargaon University for providing me such an opportunity to come closer to real situation.

Finally, I want to express my deep gratitude to my family members and all well wishers whose enormous helps assisted me to complete this Research.

MD Naim Uddin
ID No: LLB 2102023025
Batch-23rd
Department of Law
Sonargaon University

ABSTRACT

In the digital era, the balance between national security and the right to privacy has emerged as a critical legal and ethical dilemma. This comparative study examines the national security legislation of the United States, the United Kingdom, and India, focusing on how each nation addresses surveillance, data protection, and individual privacy in the face of growing security threats. The analysis explores key laws such as the USA PATRIOT Act and FISA in the U.S., the Investigatory Powers Act in the U.K., and India's Information Technology Act and Personal Data Protection frameworks.

While these laws empower governments to counter terrorism and cybercrime, they also raise significant concerns about mass surveillance, lack of judicial oversight, and the erosion of fundamental rights. The study highlights common challenges, including overbroad state powers, inadequate transparency, and insufficient safeguards for citizens. Drawing lessons from these jurisdictions, the research underscores the need for a rights-based approach that harmonizes security imperatives with robust legal protections for privacy. The findings call for reform measures including enhanced oversight mechanisms, data minimization principles, and stronger constitutional safeguards to ensure accountability and uphold democratic values in the digital age.

TABLE OF CONTENTS

Chapter : Five
Right to Privacy in the U.K

Chapter : Six
Protection of Right to Privacy

Chapter : Seven
Suggestions and Conclusion

Chapter 1
Introduction

1.1 Introduction

In the digital age, the intersection of national security and the right to privacy has become one of the most pressing legal and ethical issues faced by modern democracies. As states grapple with emerging threats such as terrorism, cybercrime, and cross-border extremism, governments around the world have enacted expansive national security legislation to enhance surveillance, intelligence gathering, and data retention capabilities. However, these efforts often raise serious concerns about the infringement of individual privacy rights, particularly in a world increasingly reliant on digital communication and information technologies.

The United States, the United Kingdom, and India—three major democracies with diverse legal systems and political contexts—have each developed their own frameworks to address national security in the digital realm. Laws such as the USA PATRIOT Act and Foreign Intelligence Surveillance Act (FISA) in the U.S., the Investigatory Powers Act in the U.K., and India's Information Technology Act and Personal Data Protection Bill reflect a global trend of expanding state power in the name of security. Yet, these laws have sparked debates about mass surveillance, lack of transparency, and the potential erosion of civil liberties.

This study aims to conduct a comparative analysis of national security legislation in these three countries to evaluate how effectively they balance the imperatives of state security with the fundamental right to privacy. By examining legal texts, judicial decisions, and oversight mechanisms, the research seeks to uncover common challenges, best practices, and avenues for reform. In doing so, it contributes to the broader discourse on how democratic societies can uphold both safety and freedom in an era defined by digital interconnectivity and increasing geopolitical uncertainty.

Poverty is relative, and the lack of food and of the necessities of life is not necessarily a hardship. "Spiritual and social ostracism, the invasion of your privacy, are what constitute the pain of Poverty The terra "privacy" is used frequently in ordinary language as well as in philosophical, political and legal discussions, yet there is no single definition or analysis or meaning of the term. The concept of privacy has board historical roots in sociological and

anthropological discussions about hew extensively it is valued and preserved in various cultures. Moreover, the concept has historical origins in well known philosophical discussions, most notably Aristotle's distinction between the public sphere oil political activity and the private sphere associated with family and domestic life .Yet historical use of the term is not uniform, and there remains confusion over the meaning, value and scope of the concept of privacy.[1]

Nevertheless, most theorists take the view that privacy is a meaningful and valuable concept Philosophical debates concerning definitions of privacy became- prominent in the second half of the ˉtwentieth century, and arc deeply affected by the development of privacy protection in the law. Some defend privacy as focusing over information about oneself while others defend it as a broader concept required' for human dignity or crucial for intimacy. Other commentators defend privacy as necessary for the development of varied and meaningful interpersonal relationships , or as ;he value that accords us the ability to control the access others have to us or as a set of norms necessary not only to control access but also to enhance personal expression and choice , or some combination of these. Discussion of the concept is complicated by the fact that privacy appears to be something we value to provide a sphere within which we can be free from interference by others, and yet it also appears to function negative as the cloak under which one can hide domination, degradation, or physical harm to women and others.[2]

1.2 Definition of Privacy

The term privacy is used frequently on ordinary language as well as in philosophical, political and leg discussions, yet there is no single definition or analysis or meaning of the term. The concept of privy has broad historical roots in sociological and anthropological discussions about how extensively valued and preserved in various discussions, most notably Aristotle's distinction between the sphere of political activity and the private sphere associated with family and domestic life. Historical use of the term is not uniform and there remains confusion over the scope of the concept of privacy.[3]

1 [http://www. Plato stanford.edu/ entries/ Privacy, last visited on 15.02.2017].

2 *Ibid.*

3 [http://www.definitions.uslegal.com/right-to privacy, last visited on 16.02.2017].

The right to privacy is the right to be let alone in the absence of some 'reasonable' public interest in a 1JJ' person's activity, like those of celebrities or participation in newsworthy events. Invasion of the right to privacy can be the basis for a lawsuit for damages against the person or entity violating the right.

The privacy right is not mentioned in the constitution, but the Supreme Court has interpreted several of the amendments as creating this .One of the amendments is the Forth Amendment ,which stops me police and other government agents from searching us or our property without 'probable cause' to believe that we have committed a crime. Other amendments protect our freedom to make certain decisions about our bodies and our private lives without interference from the government. The -due process clause of 14^{lh} amendments generally only protects privacy of family, marriage .motherhood, procreation and child rearing.[4]

1.3 Purpose of the Research

The primary purpose of this research is to critically examine the evolving relationship between national security legislation and the right to privacy in the digital era, with a comparative focus on the United States, the United Kingdom, and India. In an age where governments increasingly rely on digital surveillance and data collection to combat terrorism, cyber threats, and other security challenges, this study aims to understand how legal frameworks in these three countries balance state security interests with individual privacy rights.

Specifically, the research seeks to:

1. Analyze key national security laws and their implications for digital privacy.
2. Identify the extent to which these laws conform to constitutional and international human rights standards.
3. Explore the mechanisms of oversight, accountability, and transparency in surveillance practices.
4. Draw comparative insights that highlight best practices and potential legal reforms.
5. Recommend policy measures to ensure that national security objectives do not unjustifiably infringe upon the fundamental right to privacy.

---

4 *Ibid.*

By doing so, the study aspires to contribute to the global discourse on digital rights and inform the development of balanced, rights-respecting legal regimes that protect both national interests and civil liberties.

1.4 Research Questions

This study is guided by the following key research questions:

1. How do the national security legislations of the U.S., U.K., and India address surveillance and data collection in the digital era?
2. To what extent do these laws safeguard or compromise the right to privacy of individuals in each jurisdiction?
3. What legal and institutional mechanisms exist to ensure accountability, oversight, and transparency in state surveillance practices?
4. How do constitutional protections and judicial interpretations in the U.S., U.K., and India shape the balance between national security and privacy rights?
5. What similarities and differences can be identified in the approach of these three countries towards reconciling security and privacy?
6. What lessons can be drawn from the comparative analysis to inform legal and policy reforms that promote both national security and individual privacy?

These questions aim to uncover the legal, ethical, and practical dimensions of digital surveillance laws and contribute to the development of more balanced and rights-respecting national security frameworks.

1.5 Significance of the Study

The significance of this study lies in its critical examination of the growing tension between national security imperatives and the right to privacy in the digital age. As governments around the world expand their surveillance capabilities to address emerging threats such as cybercrime, terrorism, and transnational extremism, concerns about the erosion of civil liberties—particularly the right to privacy—have become increasingly urgent.

By focusing on the legal frameworks of the United States, the United Kingdom, and India, this research offers a comparative perspective that highlights both the common challenges and unique approaches taken by democracies with differing legal systems and socio-political contexts.

It provides insights that can inform policymakers in crafting balanced laws that protect national security without undermining fundamental rights. It enhances understanding of how existing legislation aligns or conflicts with constitutional and international human rights standards. The comparative nature of the study allows for cross-jurisdictional learning, offering lessons that may be applicable to other countries facing similar dilemmas. It contributes to the growing body of literature on digital rights, constitutional law, and the governance of surveillance technologies. By shedding light on the implications of national security laws, the study promotes public discourse and civic engagement around privacy and accountability in a digital society.

1.6 Statement of the Problem

In the digital era, the rapid advancement of technology has significantly transformed the landscape of national security and law enforcement. Governments now possess unprecedented capabilities to collect, store, and analyze vast amounts of personal data in the name of national security. However, this expansion of surveillance powers has raised serious concerns regarding the infringement of the fundamental right to privacy.

The core problem lies in the growing tension between ensuring national security and safeguarding individual privacy rights. In countries like the United States, the United Kingdom, and India, legal frameworks such as the USA PATRIOT Act, the Investigatory Powers Act, and India's Information Technology Act have enabled mass surveillance and data interception practices. While these measures aim to prevent terrorism and enhance security, they often lack sufficient judicial oversight, transparency, and accountability, potentially leading to abuse of power and erosion of civil liberties.

Moreover, the absence of uniform privacy standards, unclear data protection mechanisms, and inconsistent judicial interpretations across jurisdictions further complicate the matter. Citizens are increasingly vulnerable to intrusive state practices without adequate legal remedies or protections.

This research addresses the urgent need to evaluate whether existing national security legislation in these countries appropriately balances the legitimate interests of security with the protection of privacy rights. The problem is both legal and ethical, calling for a nuanced

understanding of how democratic societies can uphold security while maintaining the rule of law and fundamental freedoms in the digital age.

1.7 Scope of the Study

This study undertakes a comparative legal analysis of national security legislation and the right to privacy in the digital era, focusing specifically on three democratic countries: the United States, the United Kingdom, and India. It examines the evolution, content, and implementation of key legal instruments such as the USA PATRIOT Act and Foreign Intelligence Surveillance Act (FISA) in the U.S., the Investigatory Powers Act in the U.K., and the Information Technology Act, along with emerging data protection frameworks in India. The study explores how these laws facilitate digital surveillance, data retention, and intelligence gathering, and how they impact the constitutional or human rights protections of individual privacy.

The analysis includes:

- Legal frameworks and their constitutional compatibility
- Institutional mechanisms for oversight and accountability
- Relevant judicial decisions and interpretations
- Comparative best practices and reform initiatives

1.8 Limitations of the Study:

- **Jurisdictional Focus:** The research is limited to the U.S., U.K., and India and does not cover other countries or regional frameworks such as the EU's GDPR in depth.
- **Time Frame:** Given the rapidly evolving nature of digital technology and surveillance tools, some legislative developments or judicial rulings may occur after the completion of this study and thus remain unaddressed.
- **Technical Scope:** The study emphasizes legal and policy analysis rather than the technical or operational dimensions of surveillance technologies.
- **Access to Data:** Some surveillance practices and intelligence operations are classified or opaque, limiting access to complete and verifiable information.
- **Comparative Challenges:** Differences in legal systems (common law vs. statutory law), institutional structures, and political cultures may complicate direct comparisons.

Chapter 2

Right to Privacy in Bangladesh

2.1 Privacy Law in Bangladesh

Privacy is a fundamental human right. It underpins human dignity and other values such as freedom of association and freedom of speech. It has become one of the most important human rights of the modern age.

"Article 43 of the constitution says that every citizen shall have the right to privacy of his correspondence and other means of communication.[5] Now there is no means to ensure this right to citizens we get phone calls from superstores .marketing firms and other organizations who are not supposed to have our contract information and yet they have other names .phone numbers and family information all without our consents. Phone are tapped in the name of security .emails are scrutinized and correspondences are' monitored by security agencies .We even had to rive our fingerprints to the state for the national identity card These are nothing but criminalizing the society, only convicted criminals in the US are required to give their fingerprints to the state, but here in Bangladesh .every citizen is required to give their fingerprints for the national identity card and simcard registration .This is blatant violation of individual privacy .In return of privacy the state with information ,the citizens are not receiving any kind of benefits as well.

The real problem lies in the society mindset where no one is aware of rights to individual privacy. Our children are bought up in an environment where they are not given any privacy or individual freedom .So they DO not understand the value of privacy .Information is an asset and it need to be protect. It is difficult to ensure protection of individual privacy and personal information, the discussants added.[6]

---

[5] *The Constitution of the people's Republic of Bangladesh, 1972.*

6)MD.Zahidul Islam and Asma jahan,[''Right to privacy:] Journal of Asian and African social science

And Humanities, vol-1,no-1:1-7,2015 … AND S.M. Masum Billah, 'Right to Privacy: Philosophical Prelude, Development and

Challenges.' Mizanur Rahman, Ed.,*HRSS Manual*,(Dhaka: ELCOP,2006).

2.2 Right to privacy in Bangladesh Constitution

The Constitution of Bangladesh (Bangle; Bangladesh Shongbidhan) is the supreme law of Bangladesh, it declare-

Article 31 Right to Protection of Law

To enjoy the protection of the law, and to be treated in accordance with law, and only in accordance with law, is the inalienable right of every citizen, wherever he may be, and of every other person for to the time being within Bangladesh, and in particular no action detrimental to the life, liberty, body,. Reputation or property of any person shall be taken except in accordance with law. (Underline marked |, by the author)

Article 32 Protection of Right to Life and Personal Liberty

No person shall be deprived of life or personal liberty, save in accordance with law.

Article 42 protection of right to property

Subject to any restrictions imposed by law ,every citizen shall have the right to acquire,hold,transfer,or otherwise dispose of property,and no property shall be compulsorilyaquired,nationalized or requisitioned save by authority of law.

Article 43 Protection of Home and Correspondence

subject to any reasonable restrictions imposed by law in the interne *jurist* of the State, public order, public morality or public health-in his home against entry, search and seizure; and the privacy of his correspondence and other means of communication.[7]

2.3 To privacy in Bangladesh: Some Instances

communication and information sharing, the Internet hasalso facilitated the development of large amounts of transactional data by and about individuals. This information, known as communications data or metadata, includes personal information on individuals, their location and online activities, and logs and related information about the e-mails and messages they send or receive." This communications data is "storable, accessible and searchable," and when it is combined and aggregated and used by the state, it can be "both highly revelatory and invasive."Ever since electronic media were opened to private sector involvement in the early 1990s, successive Bangladeshi governments have encouraged the development of an open internet access and communication regime in the country. Bangladesh currently has 33 million internet users, representing almost 20% of the total population, and ranks 138th out of 190 countries in the world. The World Economic Forum's

7) The Constitution of the people's Republic of Bangladesh, 1972.

2013 Global Information Technology Report ranked Bangladesh 114th out of 144 countries worldwide, with poor scores for its infrastructure and regulatory environment, even though an affordable and competitive communication service is generating exponential growth for users.[8] In addition, localisation and the availability of phonetic Bangla software have contributed to the development of local blog and content hosting services.The current government in Bangladesh has a plan to establish what it calls a "Digital Bangladesh by 2021", with the aim of integrating internet access with development efforts in various sectors. But with widespread digital communication comes a greater threat to security and privacy, and uncertainty on how state and other institutions will address those issues while protecting the rights of individuals. Globally there are two models available to protect citizens. One is the authoritarian model, where the problem is addressed through the development of a surveillance regime with filtering at the control points or on the backbone of the internet, and monitoring of the use of computers. A more liberal approach, on the other hand, is to make people aware of the risks, to develop their capacities and to set down punitive measures that require proper evidence and respect individual rights. Bangladesh is often swinging between these two models, and there is a sense in which it is addressing the situation on an ad hoc basis.Communication content can reveal a range of sensitive information about an individual, including a person's identity, behaviour, associations, physical and medical data, race, colour, sexual orientation, national origins and viewpoints. Or it can show trends in a person's location, movements, interaction or behaviour patterns over a period of time through metadata or other forms of data associated with the original content. Therefore, this requires significant protection in law.Internationally, regulations concerning government surveillance of communications vary in approach and effectiveness, often with very weak or non-existent legal safeguards. The Constitution of Bangladesh touches on the issues of privacy and individual security in several places. Article 11says that the republic shall be a democracy in which fundamental human rights and freedoms and respect for the dignity and worth of humans shall be guaranteed. Article 43 states that every citizen has the right to be secured in his or her home against entry, search and seizure, and the right to the privacy of his or her correspondence and other means of communication, unless there are any reasonable restrictions imposed by law in the interests of the security of the state. In Bangladesh cyber crime is addressed with reference to several laws, including the Information and

[8]) [Global Information society watch 2014] and The Daily Star report.

Communication Technology Act, 2006; the Penal Code,1860; the Pornography Act, 2012; and the Bangladesh Telecommunication Act, 2001. The Bangladesh Telecommunication (Amendment) Act, 2006, allows agencies to monitor the private communications of people with the permission of the chief executive of the Ministry of Home Affairs, under a special provision for the security of state and public order. This act was again amended in 2010, enabling officials to intercept the electronic communications of any individual or institution in order to ensure the security of the state or public order.The act was further amended in 2013 by granting law enforcers the right to arrest any person without warrant, and by making the crimes nonbailable. Section 57 of the ordinance states that if any electronically published material causes any deterioration of law and order, tarnishes the image of a person or the state, or hurts the religious sentiment of people, then the offender will be punished for a maximum of 14 years imprisonment.The Bangladesh Telecom Regulatory Commission (BTRC) also has the authority to tap and monitor phone calls if deemed necessary. The commission's International Long Distance Telecommunications System Policy has enabled the country to set up three private international gateways, six interconnection exchanges and one international internet gateway. This policy says the operators of these will arrange the connection, equipment and software needed for online and offline monitoring, and will provide access for "lawful interception" by law enforcement agencies. All operators are also required to provide the records of call details (voice and data) whenever necessary. The BTRC may also set up a monitoring centre at the country's submarine cable landing station which connects Bangladesh's internet backbone to the rest of the world. In January 2012, the BTRC created an 11-member Bangladesh Computer Security Incident Response Team (BD-CSIRT) to look into the issues of cyber crime. This team was mandated to use wiretapping and internet surveillance if necessary. The government has also set up a "cyber tribunal" as per Section 68 of the ICT Act of 2006 to deal with cyber crime-related issues. The Right to Information Ordinance of 2008 was modified and gazetted in 2009. This ordinance has a provision for the proactive disclosure of information ensuring better transparency in the administration, but the amended ICT Act of 2013 may discourage the administration to disclose any information fearing the application of Section 57 of ICT Act.As discussed, the legal framework (such as the ICT Act and its 2006 and 2010 amendments) allows law enforcement agencies to monitor and intercept private communication. Therefore, communication surveillance probably happens at a level we are not aware of. There was a report recently that Bangladesh is buying advanced communication surveillance equipment,

which certainly validates this supposition. This Came out more publicly in 2007 when, in a circular, the BTRC requested all internet service providers (ISPs) to submit the names, addresses, logins, location and other usage statistics of their users. What they did with that information is still unknown. It has been reported that the BTRC often serves informal orders to different domestic service providers to provide information or block certain content – the ISPs are legally bound to do this through their licence and operations agreements with the BTRC. However, there is the problem of cyber crime too. For example, a number of district web portals that were inaugurated by the prime minister in January 2010 were hacked immediately afterwards.Different government and media websites, including those of leading newspapers, are attacked quite frequently.The use of social media is growing exponentially. Facebook, for example, is one of the most visited websites in the country, attracting more than 10% of the nation's total internet users. The platform or different pages within the platfom has been blocked several times in Bangladesh. In 2013 a Facebook report showed that the Bangladeshi government requested the profile information of 12 users. A newspaper report suggests that the government asked Facebook on three occasions to remove content from its site. Popular video platform YouTube has been blocked repeatedly in recent times. First it was blocked in March 2009 after a recording of a meeting between the prime minister and army officers was published on the site. The block was lifted several days later. YouTube was blocked again in September 2012 following a controversial video clip on Islam – the block was later lifted in June 2013. Although the reason given for the latter block was that the post hurt religious sentiment, many believe that the actual purpose was to exert more control over online content and behaviour. What was more worrying was the perspective of a Bangladeshi court which expressed the desire to find ways of facilitating future blocks of websites and pages. The court ordered the shutdown of five Facebook pages and a website for content deemed blasphemous towards Islam, while demanding that content hosts and creators be brought to justice for "uploading indecent material."Hurting religious sentiment is increasingly becoming a major issue when it comes to surveillance. Authorities seem to be ill prepared, both at the policy and implementation level, to define the issue properly. In October 2012, in the southeastern district of Ramu, temples in Buddhist neighbourhoods were attacked and vandalised following an allegation that the Facebook profile of a Buddhist showed an anti-Islamic image, inciting local Muslims to retaliate. Similarly, in another incident in November 2013, vandals attacked Hindu houses and properties claiming that a local Hindu boy had uploaded something derogatory towards Islam on his Facebook profile,

although this was later denied by the person in question.Social media played an important role in mobilising tens of thousands of people who gathered at Shahbagh Square in Dhaka in February 2013.[8] This was in protest against a light court sentence given to Abdul Qader Mollah, an alleged war criminal of the 1971 liberation war. Social, cultural and pro-independence political forces later joined and strengthened the non-violent demonstration, causing some observers to compare it to the 2011 protests in Egypt's Tahrir Square. But, in response, Mollah's supporters rallied against what they called a conspiracy by "atheist bloggers". On 15 February 2013 armed assailants followed, attacked and killed a blogger, one of the organisers of the Shahbagh demonstration, outside of his home. This shows how people see security threats as linked to online activism, and how surveillance and monitoring are also happening between citizens. Many argue that the government uses security as an excuse to tame dissenting voices, and Section 57 of the ICT Amendment Act of 2013 gives enough power to the government to arrest and confine anyone without a warrant.[9] Online activists are already finding themselves in an uncomfortable zone regarding the ICT Act amendment, and the ways in which it allows surveillance of communications. In one instance, a professor at a public university was sentenced to a six-month jail term by a court for failing to appear in court (due to the fact that he was in Australia at the time) to stand trial regarding his Facebook statement against the prime minister.In another incident, a college student was arrested after posting some "derogatory comments" about the prime minister and her late father, Bangladesh's founding leader, Sheikh Mujibur Rahman. No wonder the government's response was to create the BD-CSIPT to identify the websites and persons or institutions that engage in activities that can be seen as harmful to the state, society, political and religious beliefs whether using mobile phones, a simple website, or social media.Bangladesh still does not have any proper legal framework to protect privacy rights and to counteract surveillance. Communication surveillance happens both officially and unofficially without muchchallenge. Civil society has a bigger role to play in this context. Civil society organisations can raise awareness among citizens and can push the government to educate and empower people on issues of privacy, cyber crimes, etc. This is preferable to the authoritarian approach of blocking or filtering content, or conducting surveillance. A comparative study on what other countries specially(India and USA) have done and what they have achieved could be a useful

[8] Donohue, L. K. (2016). *The Future of Foreign Intelligence: Privacy and Surveillance in a Digital Age*. Oxford University Press.

[9])Ict act of Bangladesh 2001,2006,2010,and 2013(last amendment Act)

background resource to create this awareness and understanding. Activists can prepare guidelines on user rights and obligations and what can be done if someone feels violated by communication surveillance. Civil society also needs to speak up on the unconstitutional provisions in the ICT Act amendment and other legal provisions that allow surveillance[10]

[10])[Http:www.Ifex.org/Bangladesh/2014/05/05/sequrity_Agency_Surveillance]

Chapter 3

Right to Privacy in India

3.1 Right to Privacy in Indian Constitution

Article 21 of the constitution confers the right to privacy on the citizens. This is not expressly mentioned in it but the same has been enunciated by way of judicial interpretation by the Supreme Court. It is personal in nature and only the concerned citizens has a right to control it subject to the restrictions imposed by the law, India is a signatory to the international covenant on civil and political rights, 1966.

Article 17 thereof provides for the right of privacy. Article 17 of the international covenant does not go contrary to any part of our municipal law. Article 21 has, therefore, to be interpreted in conformity with the international law. In *Kharak Singh v. State of UP* (1963) justice Subba Rao, while expressing .the minority view, laid down the foundations for the development of law of privacy in India and observed that the concept of liberty in article 21 was comprehensive enough to include privacy.[9]

In *Govind v. State of MP* (1975) the Supreme Court observed that right to privacy must encompass and protect the personal intimacies of the home, the family, marriage, motherhood, procreation and child bearing. In *R. Raja gopal v. State of TN* (1994) the Supreme Court held that the right to privacy is a right to be let alone. None can publish anything concerning the above matters without his consent, whether truthful or otherwise and whether laudatory or critical. If he does so, he would be violating the right to privacy of the person concerned and would be liable in an action for damages.

In *P.U.C.L. v. Union of India* (1996) [31]the Supreme Court held that the right to hold a telephone conversation in the privacy of one's home or office without interference can certainly be claimed as-right to privacy. Telephone tapping would, thus, infringe article 21 of the constitution of India. In *Mr. X v. Hospital Z* (1998) the Supreme Court held that the right to privacy may, apart from contract, also arise out of a particular specific relationship, which may be commercial, matrimonial or even political. Public disclosure of even true private facts may amount to an invasion of the right to privacy.[10]

[9] Lyon, D. (2018). *The Culture of Surveillance: Watching as a Way of Life*. Polity Press.

11. Md. Ershadul Karim, "citizen Right to privacy:Reflection in international instrument and Natural Laws, "Bangladesh Journal of Law,vol 9 no 1&2(2005)p.38-45

The constitution of India provides fundamental rights under chapter III. those right are grunted by the constitution. One of these rights is provided under article 21 which reads as follows:-

Article 21 Protection of Life and Personal Liberty: No person shall be deprived of his life or "personal liberty except according to procedure established by law. [11]

Though the phraseology of Article 21 starts with negative word but the word No has been used in "relation to the word deprived. The object of the fundamental right under Article 21 is to prevent encroachment upon personal liberty and deprivation of life except according to procedure established by law. It clearly means that this fundamental right has been provided against state only; If an act of private individual amounts to encroachment upon the personal liberty or deprivation of life of other person. Such violation would not fall under the parameters set for the Article 21. In such a case the remedy for aggrieved person would be either under Article 226 of the constitution or under general law.[12] But, where an act of private individual supported by the state infringes the personal liberty or life of another person, the act will certainly come under the ambit of Article 21. Article 21 of the Constitution deals with prevention of encroachment upon personal liberty or deprivation of life of a person.

The state cannot be defined in a restricted sense. It includes Government Departments, Legislature, Administration, Local Authorities exercising statutory powers and so on so forth, but it does not include nor.-statutory or private bodies having no statutory powers. For example: company, autonomous body and others. Therefore, the fundamental right guaranteed under Article 21 relates only to the acts of State or acts under the authority of the State which are not according to procedure established by law. The main object of Article 21 is that before a person is deprived of his life or personal liberty by the State, the procedure established by law must be strictly followed. Right to Life means the right to lead meaningful, complete and dignified life. It does not have restricted meaning. It is something more than surviving or animal existence. The meaning of the word life cannot be narrowed down and it will be available not only to every citizen of the country. As far as Personal Liberty is concerned, it means freedom from physical restraint of the person by personal incarceration or otherwise and it includes all the varieties of rights other than those provided under Article 19 of the Constitution. Procedure established by Law means the law enacted by the State. Deprived has also wide range of meaning under the Constitution, These ingredients

---

[12] .The Indian Constitution,1949.

are the soul of this prevision. Fundamental right under Article 21 is one of the most important rights provided under the Constitution have been described as heart of fundamental rights by the Apex Court.[11]

The scope of Article 21 was a bit narrow till 50s as it was held by the Apex Court in Goalies case that the contents and subject matter of Article 21 and 19 1) (d) are not identical and they proceed on total principles. In this case the word deprivation was construed in a narrow sense and it was held that the deprivation does not restrict upon the right to move freely which came under Article 19 (1) (d). at that time Goalies case was the leading case in respect of Article 21 along with some other Articles of the Constitution, but post Copeland case the scenario in respect of scope of Article 21 has been expanded or modified gradually through different decisions of the Apex Court and it was held that interference with the freedom of a person at home or restriction imposed on a person while in jail would require authority of law. Whether the reasonableness of a penal law can be examined with reference to Article 19, was the point in issue after Complain case in the case of *Maneka Gandhi v. Union of India,* the Apex Court opened up a new dimension and laid down that the procedure cannot be arbitrary, unfair or unreasonable one. Article 21 imposed a restriction upon the state where it prescribed a procedure for depriving a person of his life or personal liberty. This view has been further relied upon in a case of *Francis Coralie Mullin v. The Administrator,* Union Territory of Delhi(1981) and others as follows:

Article 21 requires that no one shall be deprived of his life or personal liberty except by procedure established by law and this procedure must be reasonable, fair and just and not arbitrary, whimsical or fanciful. The law of preventive detention has therefore now to pass the test not only for Article 22, but also of Article 21 and if the constitutional validity of any such law is challenged, the court would have to decide whether the procedure laid down by such law for depriving a person of his personal liberty is reasonable, fair and just. In another case *of Olga tellis and others v. Bombay Municipal Corporation and others(1992)*[13]. it was further observed : Just as a fide act has no existence in the eye of law, even so, unreasonableness vitiates law and procedure alike. It is therefore essential that the procedure prescribed, by law for depriving a person of his fundamental right must conform the norms of justice and fair play. Procedure, which is just or unfair in the circumstances of a case, attracts the vice of unreasonableness, thereby vitiating the law which prescribes that procedure and consequently, the action taken under *it. As stated* earlier, the protection of Article 21 is wide enough and it was further widened in the case of *Bandhua Mukti Morcha v. Union* of India

and others(1984) in respect of bonded lab our and weaker section of the society[13]. It lays down as follows:

Article 21 assures the right to live with human dignity, free from exploitation. The state is under a constitutional obligation to see that 'there is no violation of the fundamental right of any person, particularly when he belongs to the weaker section of the community and is unable to wage a legal battle against a strong and powerful opponent who is exploiting him. Both the Central Government and the State Government are therefore bound to ensure observance of the various social welfare and lab our laws enacted by Parliament for the purpose of securing to the workmen a life of basic human dignity in compliance with the directive principles of the state policy.

The meaning of the word life includes the right to live in fair and reasonable conditions, right to rehabilitation after release, right to live hood by legal means and decent environment. The expanded scope of Article 21 has been explained by the Apex Court in the case of Unni Krishnan v. State of A.P.(1993)[13] and the Apex Court itself provided the list of some of the rights covered under Article 21 on the basis of earlier pronouncements and one of them are listed below:

(1) The right to privacy.

It was *observed in Unni Krishnan's* case that Article 21 is the heart of Fundamental Rights and it has extended the Scope of Article 21 by observing that the life includes the education as well as, as right to education Haws from the right to life.[13]

3.2 Statutory rights of Citizens

The Fundamental and Constitutional rights are supplemented by certain statutory rights. The statutory rights of nations can be grouped as:

(a) Personal rights, and

(b) Proprietary rights

(a) Personal rights

The statutory law of privacy is the recognition of the individual's right to be let alone and to have his space inviolate. It is scattered in various statutes and is not recognized as such. For instance section 228A of Indian Penal Code, 1860 (IPC) prohibits the disclosure of the identity of a victim. Similarly, the Information Technology Act, 2000 (IT Act, 2000) also

[13] [http://www.indiankanoon.org>search>cases,last visited on 20.02.2017]

contains provision for the •vindication of privacy rights. For instance, if a person authorized under the act, rules or regulations, secures access to any electronic record, information, document etc without the consent of the person, concerned and discloses the same to any other person then he shall be punished with imprisonment up to 2 years, or with fine up to Rs.1 lakh or with both [2].

The following provisions of the IT Act, 2000 reflect India's concern for protection of privacy rights of its citizens, as available against private individuals, in the realm of information technology:

1. ***Long Arm Jurisdiction***

   Section 1 read with Section 75 of the Act provides for an extra-territorial application of the provisions of the Act. Thus, if a person (including a foreign national) contravenes the privacy of an individual by means of computer, computer system or computer network located in India, he would be liable under the provisions of the Act.

2. ***Unauthorized Use***

   If a person makes an unauthorized use of the computer, computer system or computer network of another person by accessing, downloading, introducing computer contaminant, damaging, disrupting, denying access etc, he will automatically violate the privacy of the owner. Such a person shall be liable to pay compensatory damages not exceeding rupees one corer to the person so affected. Thus, the right to privacy includes the right of an individual to be free from restrictions or encroachments on his person or property, whether these are directly or indirectly brought about by calculated measures.

3. ***Computer Tampering***

   The privacy of a person will also be intruded if his computer source documents arc tampered with. The person tampering with such computer source documents shall be punishable with imprisonment up to 3 years or with fine, which may extend up to Rs.2 lakes, or with both.

4. ***Computer Hacking***

   If a person causes wrongful loss or damage to any person., by destroying, deleting or altering any information residing in his (owner's) computer resource or diminishes its value or utility or affects it injuriously by any means, he commits hacking and thus, violates the privacy of the owner. The person hacking shall be punishable with imprisonment up to 3 years or with fine, may extend up to Rs.2 lakes, or with both.

However, an innocent infringer will not be liable *that* he committed the act without any intention or knowledge.

5. ***Network Service Provider's Liability***

   A network service provider shall be liable for violation of privacy of a third party if he makes available any third party information or data to a person for the commission of an offence or contravention. A citizen has a right to safeguard the privacy of his own, this family, marriage, procreation, motherhood, childbearing and education among other matters. None can publish anything concerning the above matters without his consent, whether truthful or otherwise and whether laudatory or critical. If he does so, he would be violating the right to privacy of the person concerned and would be liable in an action for damages However, a network service provider will not be liable if he proves that the offence or contravention was committed without his knowledge or he had exercised all due diligence to prevent such commission

6. ***Liability of Companies***

   Where the privacy rights of a person are infringed by a company, every person who at the time of contravention was in charge of and was responsible to the company for the conduct of its business as well as the company shall be guilty of the contravention and liable to be processed against and punished accordingly. However, such person shall not be liable if he proves that the contravention took place without his knowledge or that he exercised all due diligence to prevent such contravention. These provisions provide sufficient protection against privacy violations by private individuals by misusing the information technology.[14]

(b) Proprietary rights

The proprietary rights, in the form of data property, are available under both the Trade Related Aspects of Intellectual Property Rights (TRIPS) Agreement and the Indian Copyright Act, 1957.

The TRIPS Agreement recognizes the protection of data property in Article 10(2) of the TRIPS Agreement. Article 10(2) of the Agreement provides that compilation of data or other material, whether in machine-readable or other form, which by reason of the selection or arrangement of their contents constitute intellectual creations shall be protected as such. The Article further provides that such protection, which shall not extend to the data or material

[14][Information Technology Act,2000 of indian constitution.and amendment act 2008]

itself, shall be without prejudice to any *subsisting* in the data or material itself. A closer perusal of the Article reveals following bets;

i. It is the compilation of data or other material which is protected under TRIPS Agreement. The Compilation of a subject matter of Copyright is protected under almost all the legal systems. This is also protected in the Berne Convention. Further, by using the words other materials the ambit of this Article has been extended to even non-data items.

ii. The compilation may be either in 2 machine-readable forms or in some other form. The previous category includes storing of data in computers and its parallels, whereas the latter category includes storing of the data in the traditional paper mode. This storing of data property mandates protection of the same in IT law as wail. The Copyright Act, 1957 protects databases as literary works under section 2(o) in an inclusive manner and it can cover more categories.

Secondly, the concept of compilation used in this section is itself inclusive and the compilation of databases is one of them. Thus, compilation U/S-2(o), includes at least two forms of compilation. The one is compilations for the purpose of conferment of Copyright and the other is compilation for the purpose of Data Protection. Section 13(1) (a) of the Copyright Act uses the expression original literary works not only in an inclusive manner but also in a multifunctional manner. The copyright Act protects original compilations as both copyright and databases. It would be wrong to suggest that copyright and data protection are one and the same thing. These two are different Intellectual Property Rights, which are expressly protected not only under the TRIPS Agreement but also equally under the Copyright Act. In fact the definition of literary work is capable of accommodating other materials as well, which may be non-data in nature.

iii. The data protection originates because of the selection or arrangement of the contents by using the intellectual creations. If there is no intellectual endeavor involved in it, then the same may not boo protected as data property but as Copyright, since the protection of copyright is not dependent upon the quality of the contents but their expression as such. Thus, all databases are capable of copyright protection but not all copyrightable material qualifies for the data protection. The requirement of quality is more demanding in data property than the copyright. A material may fail to qualify for data protection, but it can still be copyrighted. This point is clarified by the use of the words as such in Article 10(2) of the TRIPS Agreement.

Thus the TRIPS Agreement and the Copyright Act, 1957 sufficiently safeguard databases. The data, action and details will get the protection of Data Property if the same involves intellectual creations within the meaning of Article 10(2) of 'the TRIPS Agreement. If not, still they will be 'protected as copyright. Even non-data items are also protected, both under the TRIPS Agreement and the Act

The following Data protection principles must be adhered to by the individuals and company handling the same:

(a) The data should be processed fairly and lawfully,

(b) The data should be obtained for specific and lawful purpose,

(c) The data should be adequate, relevant and not excessive,

(d) The data should not be kept for longer than necessary,

(e) The data should be processed in accordance with the rights of data subjects, and.

(f) Measures should be taken against unauthorized or unlawful processing. [15]

iv. Strategies for companies

The companies operating in cyberspace are at the risk of violating various laws including laws protecting privacy rights and data property. The companies must formulate sound strategies to deal with them.

The following strategies must be adopted by the companies for meeting various techno-legal requirements:

1. The companies must be cautious of the liability clause of various statutes. They must appoint an officer in default who must be responsible for managing cyber law matters of companies.
2. The web-site contracts made by the companies must be unambiguous and fair.
3. The companies must restrict their liabilities under those contracts.
4. Companies must adopt the well accepted standards of the contemporary practices.
5. The privacy rights of the citizens should be properly safeguarded.
6. Precautionary measures for the protection of valuable data, information, and trade secrets should be adopted.
7. The companies must take care of APRs violations of various segments,
8. The companies must adopt sound advertisement policy.
9. The companies must be very cautious while dealing with juveniles as they are protected by laws but not the companies,
10. The companies -must insure their business for uncertain risks.[15]

[15] Md.Ershadul Karim, p.58-61

Chapter 4

Right to Privacy in the U.S

Privacy is the expectation that confidential personal information disclosed in a private place will not be disclosed to third parties, when that disclosure would cause either embarrassment or emotional distress to a person of reasonable sensitivities. Information is interpreted broadly to include facts, images (e.g., photographs, videotapes), and disparaging opinions.

The right of privacy is restricted to individuals who are in a place that a person would reasonably expect to be private (e.g., home, hotel room, telephone booth). There is no protection for information that either is a matter of public record or the victim voluntarily disclosed in a public place. People should be protected by privacy when they "believe that the conversation is private and can not be heard by others who are acting in a lawful manner." Am.Jur.2d Telecommunications § 209 (1974).

The easiest method to keep information confidential is to disclose it to no one, but this is too severe a method, in that it forces a person to be a recluse and denies a person medical care, among other ' unacceptable limitations.[16]

4.1 History of privacy law in the U.S

Legal concepts like ownership of real property and contracts originated many hundreds of years ago or and are now well established in law. In contrast, the right of privacy has only recently received legal recognition and is still an evolving area of law. It is generally agreed that the first publication f advocating privacy was the article by Warren and Brandeis, *The Right to Privacy, 4* Harvard L.R. 193 (1890). However, the codification of principles of privacy law waited until Prosser, *Privacy,* 48 If Cal.L.Rev. 383 (I960), which Prosser subsequently entered into the Second Restatement of Torts 562A-6521(1977)[17]

4.2 Modern Privacy Law in the U.S

Because privacy is an emerging right, a discussion of privacy is typically a list of examples where the right has been recognized, instead of a simple definition. Privacy can be discussed in two different directions the nature of the right and the source of the right (e.g., case law.

[16] [http:/www.en.wikipedia.org/wiki/privacy,last visited on 10.03.2017]
[17] [http://www.rbs2.com/privacy.htm,last visited on 14.03.2017]

statute, Constitution) Prosser, in both his article and in the Restatement (Second) of Torts at §§ 652A-652I classifies four basic kinds of privacy rights:

i. unreasonable intrusion upon the seclusion of another, for example, physical invasion of a person's home (e.g., unwanted entry, looking into windows with binoculars or camera, tapping telephone), searching wallet or purse, repeated and persistent telephone calls, obtaining financial data (e.g., bank balance) without person's consent, etc.

ii. appropriation of a person's name or likeness; successful assertions of this right commonly involve defendant's use of a person's name or likeness on a product label or in advertising a produce or service. A similar concept is the "right of publicity" in Restatement (Third) Unfair Competition §§46-47 (1995). The distinction is that privacy protects against "injury to personal feelings", while the right of publicity protects against unauthorized commercial exploitation of a person's name or face. As a practical matter, celebrities generally sue under the right of publicity, while ordinary citizens sue under privacy.

iii. Publication of private facts for example, income tax data, sexual relations, personal letters, family quarrels, medical treatment, photographs of person in his/her home.

iv. Publication that places a person in a false light, which is similar to defamation. A successful defamation action requires that the information be false. In a privacy action the information is generally true, but the information created a false impression about the plaintiff.

Only the second of these four rights is widely accepted in the USA. In addition to these four pure privacy torts, a victim might recover under other tons, such as intentional infliction of emotional distress, assault, or trespass.

Unreasonable intrusion upon seclusion only applies to secret or surreptitious invasions of privacy. An open and notorious invasion or privacy would be public, not private, and the victim could then choose not to reveal private or confidential information. For example, recording of telephone conversations is not wrong if both participants are notified before speaking that the conversation is, or may be, recorded. There certainly are offensive events in public, but these are properly classified as assaults, not invasions of privacy.

Other privacy rights are contained in criminal statutes. For example,

a. Surreptitious interception of conversations in a house or hotel room is eavesdropping. See,e.g., N.Y. Penal §§ 250.00, 250-05

b. One has a right of privacy for contents of envelopes sent via first-class U.S. Mail. 18 USC § 1702; 39 USC 3623
c. One has a right of privacy for contents of telephone conversations, tiderips messages, or electronic data by wire. 18 USC § 2510 et seq.
d. One has a right of privacy for contents of radio messages. 47 USC §605
e. A federal statute denies federal funds to educational institutions Thai co act maintain confidentiality of student records, which enforces privacy rights of students in a backhanded way. 20 USC § 1232g. Commonly called the Buckley-Pell Amendment to the Family Educational Rights and Privacy Act. *See also Krebs v. Rutgers,* 797 F.Supp. 1246 (D.N.J. 1991); *Tombrello v. USX Corp.,* 763 F.Supp. 541 (N.D.Ala. 1991).
f. Records of sales or rentals of video tapes are confidential, 18 USC §2710
g. Content of e-mail in public systems are confidential. 18 USC § 2702(a).
h. Bank records are confidential. 12 USC §340! et seq.
i. Library records are confidential in some states. e.g., N.Y. CPLR § 4509: *Quad/Graphics, Inc.* v. *Southern Adirondack Library Sys.,* 664 N.Y.S.2d 225 (N.Y. Sup. Ct. 30 Sep 1997)[18]

4.3 Professional ethics in privacy

Other examples of privacy are included in professional ethics, such as confidentiality of disclosures during physician-patient, priest-penitent, attorney-client relationships, together with the evidence code that protects such disclosures. Violation of such confidentiality can be a tort, *Humphers v. First Interstate Bank of Oregon, 696* P.2d 527 (Or. 1985)(physician violated confidentiality of adoption by *helping* daughter find her birth mother). The violation of confidentiality could also be a matter for a professional licensing board.[19]

4.3.1 Invasions of private sphere by government

The privacy issue arises in a different context when the government attempts to limit the choices of individuals in various personal areas, such as use of contraception or abortion, who to marry, and the right to chose how to rear and educate their children. Some search and seizure issues can also be interpreted as supporting the individual's right to privacy, against

[18] ibid
[19] ibid

intrusions by the police. In the context of preventing governmental intrusions into personal life, Justice Brandeis of the U.S. Supreme

Court declared that the writers of the U.S. Constitution conferred .The right to be let alone — the most comprehensive of rights and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment.

It is unnecessary here to examine the question of whether a corporation is entitled to the protection of the Fourth Amendment. Although the 'right to be let alone — the most comprehensive or rights and the right most valued by civilized men,[1] is not confined literally to searches and seizures as such, but extends as well to the orderly taking under compulsion of process, neither incorporated nor unincorporated associations can plead an unqualified right to conduct their affairs in secret. While they may and should have protection from unlawful *demands* made in the name of public investigations, corporations can claim no equality with individuals in the enjoyment of a right to privacy.[20]

4.3.2 Privacy of businesses

Businesses have no right of privacy. *California Bankers Ass'n* v. *Schultz,* 416 U.S. 21, 65 (1974); *U.S.* v. *Morton Sail Co.,* 338 U.S. 632, 652 (1950); Restatement (Second) Torts, §6521, comment *c* (1977); Prosser, *Privacy,* 48 Calif. L.Rev. 383, 408-09 (1960); Am.Jur.2d *Constitutional Law* § 606 (1979). Privacy law is phrased only as an individual person's rights. However, businesses have rights analogous to the right of privacy. For example, corporate espionage might be prosecuted as an improper acquisition of a trade secret. Restatement (Third) Unfair Competition § 43 (1995). Further, trademark law holds that a business can own a product name and prevent others from using the same name, at least in the owner's territory. 1: is interesting that confidential business information is treated as a property right, while confidential personal information is not.[21]

Possible examples of privacy violations by businesses:

When the Constitution was written in 1791, the major concern of the drafters was that a powerful government could intrude on the privacy of individual citizens, hence the provisions in the Bill of Rights, specifically the Fourth and Fifth Amendments, to protect citizens from government. Today, individuals also need protection from intrusion by large corporations, but the law has been slow to provide such protections.

[20] [http://www.privacy international.org/USA,last visited on 14.03.2017]
[21] ibid.

Consider bar code scanning of products at the cashier's register of retail stores, together with input of credit card number to pay for the purchases. The credit card number can be linked with a name and address, to generate a database of information about purchases. As one hypothetical example of what could happen, consider an unmarried school teacher in a conservative state who purchases contraceptives. Since school teachers are supposed to have good moral values, and premarital sex is wrong according to some religions, the teacher could be dismissed from his/her job. I find such an invasion of privacy to be outrageous,

A person sympathetic to the consumer would conclude that the store only had the right to use the list of items purchased for its own use (e.g., inventor control planning future purchases) and the credit card data should have been used *only* to obtain payment for the total amount of the sale to the consumer. The credit card data should never have been merged with the detailed list of items purchased.[11]

A person sympathetic to the store might conclude that the act of purchasing was a public act, for which there was no reasonable expectation of privacy. The store clerk, the person who put the items in bags, of and the people in line behind the customer are likely to be unfamiliar to the customer (i.e., public place). There is no expectation of a confidential relationship, because neither the store personnel nor the other shoppers are professionals with a duty of confidentiality to the customer. Therefore, if the customer really desires privacy, he/she should shop in a store far from his/her home (perhaps by mail order where he/she is unlikely to encounter anyone who is interested in his/her purchases.[12]

Because the store receives money from selling information or, purchases of people, customer *desire* privacy arguably should pay a fee to the store to offset the store's loss of income. On the *other hand,* one can argue that the store has no legitimate right or sell such information, therefore, an) income from the sale of information is wrongful. As a second example, consider purchases of underwear. The purchases are made in a public place and the sales clerk and other customers are not professionals with a duty of confidentiality. Therefore, under current law, there is no expectation of privacy. If the customer is a famous person, the store clerk could report the type of underwear that the famous person purchased. Yet it seems obvious that such a reporting is not only a violation of the purchaser's privacy, but is also an uncivil activity that degrades society as well as embarrasses the victim.[22]

[11] Lyon, D. (2018). *The Culture of Surveillance: Watching as a Way of Life*. Polity Press.
[12] Greenleaf, G., & Waters, N. (2014). Global data privacy laws 2013: eighty-nine countries, and accelerating. *Queen Mary School of Law Legal Studies Research Paper*, (98), 1–52.
[22] ibid.

4.3.3 Privacy of garbage

The U.S. Supreme Court has ruled that the police may legally search, without a search warrant, trash or garbage that individuals put out for collection. *California v. Greenwood,* 486 U.S. 35 (1988). As explained below, search and seizure of material placed in the trash is a clear invasion of an individual's privacy and this Supreme Court holding should be overturned.

Residents commonly place their trash plastic bags and put the bags on the curb, for pickup by the municipal trash collection service. The bags themselves are opaque, commonly black or green or brown. The technology to make transparent plastic bags is well known, yet trash bags are always opaque. The color of trash bags is our first hints that people who purchase and use trash bags do not want transparent bags, since that would allow the contents to be easily seen.

The Alaska Supreme Court recognized that almost every human activity ultimately manifests itself in waste products and any individual may understandably wish to maintain the confidentiality of his refuse.

Such routinely contains many personal items, including:

Empty prescription medicine boltless, which are always labeled with the individual's name and may be labeled with the name and dosage of the drug, so that someone who searches the trash may infer the individual's medical condition. Particularly in the case of sexually-transmitted diseases or psychiatric disorder, disclosure of the individual's medical condition could cause embarrassment.

a. Credit card receipts, which have the person's name and credit card data; someone who searches the trash could use these data to order merchandise by telephone
b. letters that contain confidential information on financial, political, religious, family, or romantic topics
c. empty containers of alcoholic beverages, which could be embarrassing in a town with a substantial number of people who disapprove of alcohol for religious or moral reasons
d. Empty boxes for condoms, birth control pill packages, empty containers of spermicidal, and other contraceptive materials that could be embarrassing, but are legal to possess and use.
e. telephone invoices, with a list of all long-distance numbers called, with the date and duration of the call
f. paper indicating membership in political or religious groups

This list makes clear that there are a number of items in household trash that people routinely regard as private. When people place such personal items in an opaque plastic bag on the curb for trash collection, they are expressing their continuing expectation of privacy.[23]

4.4 Right to privacy in the U.S

Early years

The early years in the development of privacy rights began with British common law which protected "only the physical interference of life and property." Its development of tort remedies is "one of the most significant chapters in the history of privacy law." Those rights expanded to include a right broadened even further to include a basic "right to be let alone,"

Between 1850 and 1890, U.S. newspaper circulation grew 1,000 percent from 100 papers With 800.000 readers to 900 papers with more than 8 million readers. In addition, newspaper journalism became more ser sectionalist, and was termed yellow journalism. The growth of industrialism led to rapid advances in technology, one product of which was portable, hand-held, cameras, as opposed to earlier studio cameras, which were much heavier and larger. In 1884, Eastman Kodak Company introduced their Kodak Brownie, and it became a mass market camera by 1901, cheap enough for the general public. This allowed people and journalists to take candid snapshots in public places for the first time.

Samuel D. Warren and Louis D. Brandeis, young partners in a new law firm, feared that this new small camera technology would be used by the "sensationalistic press." Seeing this becoming a likely challenge to individual privacy rights, they wrote the "path breaking" Harvard Law Review article in 1890, "The Right to Privacy ".According to legal scholar Roscoe Pound, the article did "nothing less than add a chapter to our law," and in 1966 legal textbook author, Harry Kalven, hailed it as the "most influential law review article of all." as recently as 2001, in the Supreme Court case of *Kyllo v. United Slates*, 533 U.S. 27 (2001), the article was cited by a majority of justices, both those concurring ," and those dissenting.[24]

4.5 Modern Tort Law

In the United States today, "invasion of privacy" is a commonly used cause of action in legal pleadings. Modern tort law includes four categories of invasion- of privacy:

i. Intrusion of solitude: physical or electronic intrusion into one's private quarters.

[23] Beth Givens,The rights Hand BOOk,(new York:avon books,1997)
[24] ibid.

ii. Public disclosure of private facts: the dissemination of truthful private information which a reasonable person would find objectionable

iii. False light: the publication of facts which place a person in a false light, even though the facts themselves may not be defamatory.

iv. Appropriation: the unauthorized use of a person's name or likeness to obtain some benefits.[25]

4.6 Constitutional basis for right to privacy Federal

Although the word "privacy" is actually never used in the text of the United States Constitution, there are Constitutional limits to the government's intrusion into individuals' right to privacy. This is true even when pursuing a public purpose such as exercising police powers or passing legislation. The Constitution, however, only protects against state actors. Invasions of privacy by individuals can only be remedied under previous court decisions.[13]

The Fourth Amendment to the Constitution of the United states ensures that "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be ' seized." However these rights have been changed by modern court rulings. One such ruling which allowed police without a warrant to place a tracking device on a suspect's automobile and follow him without his knowledge.[14]

The First Amendment provides a right to free assembly, broadening privacy rights. The Ninth Amendment declares that the fact a right is not explicitly mentioned in the Constitution does not mean that the government can infringe on that right. The Supreme Court recognized the Fourteenth Amendment as providing a substantive due process right to privacy. This was first recognized by several Supreme Court Justices in *Griswold v. Connecticut*, a 1965 decision protecting a married couple's rights to contraception. It was recognized again in 1973 *Roe v. Wade* which invoked the right to privacy to protect a woman's right to 'an abortion.[26]

[25] http://www.Laws.Justice.gc.ca/en/cha,last visited on 15.03.2017.
[13] Government of India. (2000). The Information Technology Act, 2000. Retrieved from https://legislative.gov.in/sites/default/files/A2000-21.pdf
[14] Supreme Court of India. (2017). *Justice K.S. Puttaswamy (Retd.) vs Union of India*, Writ Petition (Civil) No. 494 of 2012.
[26] ibid

Chapter 5

Right to Privacy in the U.K

5.1 History of Privacy Law in the U.K

The development of privacy law in the United Kingdom has evolved gradually, shaped by common law traditions, European human rights frameworks, and the increasing role of digital technology. Historically, there was no explicit right to privacy in UK law. Instead, early protections emerged through the common law principle of *breach of confidence*, which allowed individuals to seek redress when personal information was wrongfully disclosed. However, this did not amount to a comprehensive privacy right.

A major shift occurred with the enactment of the Human Rights Act 1998**,** which incorporated the European Convention on Human Rights (ECHR) into domestic law. Article 8 of the ECHR guarantees the right to respect for private and family life. This provision became a foundation for developing modern privacy protections in the UK. Courts began interpreting existing laws in line with Article 8, effectively recognizing privacy as a fundamental right.

One of the landmark cases in this context was Campbell v MGN Ltd (2004)**,** where the House of Lords acknowledged a new legal doctrine: *misuse of private information*. The ruling clarified that individuals, including public figures, have a legitimate expectation of privacy, particularly in relation to medical, personal, or family matters. Subsequent cases such as Murray v Express Newspapers (2008) **and** PJS v News Group Newspapers **(2016)** further developed the law in favor of individual privacy.[15]

Statutory protections also played a crucial role. The Data Protection Act 1998, and later the Data Protection Act 2018, aligned UK law with evolving European standards, including the EU General Data Protection Regulation (GDPR)**.** These laws regulate how personal data is collected, processed, and stored, reinforcing the right to informational privacy.

However, privacy rights in the UK have faced challenges, particularly with the expansion of state surveillance. The **Investigatory Powers Act 2016** legalized wide-ranging surveillance practices, prompting concerns over the balance between national security and civil liberties.

[15] Office of the United Nations High Commissioner for Human Rights (OHCHR). (2014). The Right to Privacy in the Digital Age. Retrieved from https://www.ohchr.org

In conclusion, privacy law in the UK has transitioned from limited common law remedies to a broader, rights-based framework, influenced heavily by European law and judicial decisions. Despite progress, the balance between privacy and security remains a continuing legal and ethical debate.

5.2 Modern Privacy Law in the U.K:

Modern privacy law in the United Kingdom is characterized by a robust framework that protects individuals' personal data and private life, while balancing competing interests such as national security, freedom of expression, and public interest. It is primarily shaped by statutory law, human rights obligations, and case law developments.

1. Legal Foundations

- **Human Rights Act 1998**: Incorporates the **European Convention on Human Rights (ECHR)** into UK law.
    - **Article 8** of the ECHR guarantees the right to respect for private and family life, home, and correspondence. UK courts use this to assess whether privacy intrusions are justified and proportionate.
- **Misuse of Private Information**: Developed through case law (e.g., *Campbell v MGN Ltd*), this tort provides a civil remedy when someone's private information is disclosed without justification. It reflects the evolving recognition of privacy as a standalone legal right in common law.

2. Data Protection Legislation

- **Data Protection Act 2018 (DPA 2018)**: The core piece of legislation governing personal data in the UK, aligning with the EU's **General Data Protection Regulation (GDPR)**, now incorporated into UK law as **UK GDPR** post-Brexit.

3. Regulation of Surveillance and Communications

- **Investigatory Powers Act 2016**: Grants authorities powers to intercept communications, retain metadata, and conduct bulk surveillance for national security purposes. It includes some oversight mechanisms, such as the Investigatory Powers Commissioner, but has been criticized for its broad scope.

4. Freedom of Expression vs. Privacy

Courts continue to weigh privacy rights against press freedom and public interest. Injunctions and anonymized judgments are tools used to protect privacy while ensuring open justice.

5.3 Professional Ethics in Privacy:

Professional ethics play a crucial role in upholding privacy standards across various sectors in the UK, particularly in law, healthcare, journalism, information technology, and data management. With increasing access to sensitive personal data, professionals are expected to maintain confidentiality, act with integrity, and respect individuals' rights in line with both legal obligations and ethical principles.

In the **legal and healthcare sectors**, confidentiality is a cornerstone of professional ethics. Solicitors and medical practitioners are bound by codes of conduct—such as those from the **Solicitors Regulation Authority (SRA)** and the **General Medical Council (GMC)**—which require them to protect client and patient information, disclosing it only with consent or when legally mandated.

In the **digital and data industries**, ethical standards emphasize data minimization, transparency, and accountability. Professionals working with personal data must comply with the **UK GDPR** and the **Data Protection Act 2018**, ensuring data is collected lawfully, processed fairly, and stored securely. Ethical frameworks developed by bodies such as the **British Computer Society (BCS)** reinforce these duties, urging IT professionals to avoid misuse of data and respect user autonomy.

In **journalism**, ethical tensions often arise between privacy and public interest. The **Editors' Code of Practice**, enforced by the **Independent Press Standards Organisation (IPSO)**, instructs journalists to avoid unjustified intrusions into personal lives unless there is a compelling public interest.

Ultimately, professional ethics in privacy in the UK go beyond legal compliance. They require a proactive commitment to fairness, discretion, and human dignity. In an age of rapid technological change and mass data collection, adherence to ethical standards is essential to maintaining public trust and protecting fundamental rights.

5.4 Right to Privacy in the U.K

The right to privacy in the United Kingdom is not protected by a single, codified constitutional document but is instead upheld through a combination of common law, statutory provisions, and human rights obligations. It reflects a balance between individual autonomy and other public interests such as freedom of expression, national security, and public safety.[16]

1. Human Rights Act 1998 and Article 8 ECHR

The most significant legal foundation for privacy rights in the UK is Article 8 of the European Convention on Human Rights (ECHR), which was incorporated into domestic law through the Human Rights Act 1998. Article 8 guarantees:

"Everyone has the right to respect for his private and family life, his home and his correspondence."[17]

This provision serves as the cornerstone for challenging intrusions by the state or private entities, although the right is qualified—meaning that interference is allowed if it is lawful, necessary, and proportionate for legitimate aims (e.g., national security, crime prevention, or protection of others' rights).

2. Common Law and Case Law

UK courts have developed a tort of misuse of private information through landmark cases such as *Campbell v MGN Ltd* (2004), which recognized a distinct right to privacy under the common law. This development allows individuals to bring civil claims when private information is unjustifiably published or disclosed.

3. Data Protection Laws

The UK GDPR and Data Protection Act 2018 provide comprehensive protection of informational privacy, granting individuals rights over how their personal data is collected, processed, and stored. These laws apply to both public and private sector organizations.

---

[16] Supreme Court of India. (2017). *Justice K.S. Puttaswamy (Retd.) vs Union of India*, Writ Petition (Civil) No. 494 of 2012.

[17] European Court of Human Rights. (2021). *Big Brother Watch and Others v. the United Kingdom* (Applications nos. 58170/13, 62322/14 and 24960/15).

4. Limitations and Challenges

Despite strong legal protections, the right to privacy in the UK faces ongoing challenges from state surveillance (e.g., under the Investigatory Powers Act 2016), media intrusion, and technological developments such as AI and facial recognition.

In conclusion, the UK's right to privacy is multifaceted and evolving, grounded in both human rights law and judicial innovation, but continues to be tested by emerging digital and security concerns.

Chapter 6

Protection of Right to Privacy

There arc sonic area concerning the protecting and preserving of privacy rights of individual. In the following area right to privacy is protecting in the following ways:

6.1 Privacy Law

Privacy protection rules regulating law enforcement and national security use of personal information can be usefully understood in two distinct categories: first, substantive roles that limit access to and usage of private information and, second, procedural rules that provide safeguards to encourage compliance and ensure accountability for compliance failures. Neither the Constitution nor any statute can anticipate in advance every particular privacy issue raised by future technologies. So the evolving .balance between the government's need to intrude on the private lives of individuals in the service of its public safety mission and the requirement to maintain individual liberty has been maintained over time by providing a degree of transparency in the use of new technologies, along with accountability to rules assured by judicial and legislative oversight. As new technologies and investigative techniques come into use, courts and legislatures have the opportunity to review these advances and make assessments of their privacy impact, guided by constitutional and public policy foundations. When new privacy risks arise or when the government powers are judged to have been extended beyond the boundaries established through the democratic process, corrective action can be taken. In order for this dynamic equilibrium of privacy and public safety to be maintained, however, transparency of the investigative process and accountability to the role of law are essential. This appendix presents both the substantive constitutional foundations of privacy rights necessary for evaluating new technology, along with a consideration of transparency, accountability, and oversight mechanisms necessary to keep counterterrorism activities within view of the democratic process Privacy law is the area of law concerning the protecting and preserving of privacy rights of individuals. While there is no universally accepted privacy law among all countries, some organizations promote certain concepts be enforced by individual countries. For example, the Universal Declaration of Human Rights, article 12, states:

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, or to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks.[27]

For Europe, Article 8 of the European Convention on Human Rights guarantees the right to respect for private and family life, one's home and correspondence. The European Court of Human Rights in Strasbourg has developed a large body of jurisprudence defining this fundamental right to privacy. The European Union requires all member states to legislate to ensure that citizens have a right to privacy, through directives such as the 1995 Directive.[28]

In the United Kingdom, it is not possible to bring an action for invasion of privacy. An action may be brought under another tort ("usually breach of confidence) and privacy must then be considered under EC law. In the UK, it is sometimes a defense that disclosure of private information was in the public interest.[29]

Concerning privacy laws of the United States, privacy is not guaranteed per se by the Constitution of the United States. The Supreme Court of the United States has found that other guarantees have "penumbras" that implicitly grant a right to privacy against government intrusion, for example in *Griswold v. Connecticut* (1965). In the United States, the right of freedom of speech granted in the First Amendment has limited the effects of lawsuits for breach of privacy. Privacy is regulated in the U.S. by the Privacy Act of 1974, and various state laws.[30]

Canadian privacy law is governed federally by multiple acts, including the Canadian Charter of Rights and Freedoms, and the Privacy Act (Canada). Mostly this legislation concerns privacy infringement by government organizations. Data privacy was first addressed with the Personal Information Protection and Electronic Documents Act, and provincial-level legislation also exists to account for more specific cases personal privacy protection against commercial organizations.[31]

6.2 Privacy on the Internet

There are many means to protect one's privacy on the internet. For example e-mails can be encrypted and anonym zing proxies or anonym zing networks like I2P and Tore can be used to prevent the internet service providers from knowing which sites one visits and with whom

[27] The universal Declaration of Human Rights,1948.
[28] The European Convention on Human Rights,1950.
[29] The Data Protection Act,1998.
[30] The Privacy Act,1974.
[31] http://www.Canada Justice.ec.ca/stable/en/laws, last visited on 16.03.2017.

one communicates. Internet privacy includes the main elements; personal data private information, and individual field. The contents of internet privacy are as follows;

1. ***Tie right to know***

   Users have a right to know what information relevant to themselves is collected by the websites, what purpose the information will be used, as well as who it will be shared.

2. ***The right to choose***

   Consumers have a right to choose the use of their personal data.

3. ***Adequate security***

   The network company should guarantee the security of information and prevent unauthorized illegal access .The users have the right to request the website to take the necessary and reasonable measures to protect their personal information.

4. In addition, internet privacy should also includes the refuses right to control the information (the user has the right to decide whether to allow others to collect or use his information) and the right to request judicial relief (the user has the right to bring a civil suit against any institution or individual engaged in infringement on his privacy).[32]

6.3 Data Protection

Information privacy or data privacy is the relationship between collection and dissemination of data, technology, the public expectation of privacy, and the legal and political issues surrounding them. *The Data Protection Act*, 1998 can be a very powerful tool to help protect your right to privacy by creating a set of rules for those who handle your personal data, and giving you a number of rights over that personal data and the way it is handled. This section will provide and overview of those rules, and of what your rights are under the DPA and how you can enforce them. The DPA also provides you with a right to access personal data which is held about you, but this is covered in the Right to know section. The processing of your personal data, as well as engaging your rights under the DPA, often also engages your right to respect for your private and family life, which is protected by Article 8. This is covered in the Article 8 section. Disclosure of your personal data to third panics may also be a breach of confidence, and this is covered in the Breach of Confidence section. This section covers:

[32] the data protection act,1998.

Overview of data protection principles, Definition of Personal data, Legitimate Processing, Individual Rights, Remedies, Exemptions, Data Protection. In the EU's Data Protection Directive and Privacy Directive, privacy in the processing of personal data and the confidentiality of communications are recognized as fundamental rights that should be protected. The Privacy Directive requires member states to harmonize and ensure an equivalent level of protection of the right to privacy with respect to personal data in the electronic communication sector. Pursuant, to this, the Data Protection Directive prohibits the transfer of personal information to any country that does not have adequate privacy laws.[33]

[33] ibid.

Chapter 7

Suggestions And Conclusion

7.1 SUGGESTIONS

In the present time, public awareness is increase in the field of privacy. People are beginning to realize the value of their personal information and the danger in leaving it unprotected, privacy is an issue to be highly concerned with the following area.

1. *Technology*

Before the influence of the use of technology in the processing of personal and private information can be dealt with, it is important to briefly pay attention to the concept technology. For the purpose of this paper the definition of Van Brakel [32] will be used, namely: the j gathering, organizing, storage and distribution of information in various formats by means of computer and telecommunications techniques based on micro-electronics. Although technology has a major impact on the gathering, storage, retrieval and dissemination of information its main ethical impact relates to accessibility/inaccessibility and the manipulation of information, it creates the possibility of wider as well as simultaneous access to information. By implication, it becomes easier to access a person's private information by more people. On the other hand, a person can be excluded from necessary information in electronic format by means of a variety of security measures such as passwords. The technological manipulation of information refers, among others, to the integration of information (merging of documents), the repackaging thereof (translations and the integration of textual and graphical formats) and the possible altering of information (changing of photographic images) by electronic means.[18]

The use of technology in the processing of information can therefore not be seen as ethically neutral. Christians refers to the use of technology as a value laden process. Kluge even comments that technology has changed the ontological status of a document with accompanying ethical implications. By this he specifically refers to the manipulation of information by means of technology.

[18] Government of India. (2000). *The Information Technology Act, 2000*. Retrieved from https://legislative.gov.in/sites/default/files/A2000-21.pdf

Brown however on the other hand, indicates correctly that the ethical problems that are caused by the use of technology do not imply - as he puts it" that we should rethink our moral values".[34]

The impact of the use of technology on the privacy of people manifests itself in a variety of areas. These areas include, inter alias the following:

a. The electronic monitoring of people in the workplace. This relates to personal information as discussed earlier. This is done by so-called electronic eyes. The justification by companies for the use of such technology is to increase productivity. Stair however, in the discussion of this practice, clearly points out the ethical problem pertaining to the use of these technologies. According to him people's privacy in the workplace are threatened by these devices. It can also lead to a feeling of always being watched- the so-called panoptic on phenomenon.
b. The interception and reading of E-mail messages. This poses an ethical problem which relates to the private communication of an individual. It is technically possible to intercept E-mail messages, and the reading thereof is normally justified by companies because they firstly see the technology infrastructure (E-mail) as a resource belonging to the company and not the individual, and secondly messages are intercepted to check on people to see weather they use the facility for private reasons or to do their job.
c. The merging of databases which contains personal information. This is also known as data banking. By this is meant the integration of personal information from a variety of databases into one central database. The problem here does not in the first place arise from the integration of the information as such. The main problems include the fact that the individual is not aware of personal informational being integrated into a central database, that the individual does not know the purpose for which the integration is effected, or by whom or for whose benefit the new database is constructed and weather the information is accurate. In order to counter these problems relating to privacy and the merging of databases the American Congress passed the Computer Matching and Privacy-Protection Act in the 1980s (Benjamin) Closely related to the merging of files is the increasing use of buying cards ("frequent-shopper cards") by retail stores. Such a card a computer chip is buried that records every item purchased along with a variety of personal information of the buyer. This

[34] Technology Information Privacy code,2003.

information obtained from the card enable marketing companies to do targeted to specific individuals because the buying habits as well other personal information of people are known.

d. Another major threat to privacy is the raise of so called hackers and crackers which break into computer system (Benjamin. This coincides with the shift in ethical values and the emergence of the cyberpunk culture with the motto of "information wants to be free".

e. The development of software that makes the decoding of digital information (which can be private information) virtually impossible also poses serious legal as well as ethical questions because it can protect criminals. A good example is the development of software called Pretty Good Privacy by P Zimmerman in 1991. According to an article in the IT Review he has

developed the most complex algorithm ever invented which makes the decoding of digital information virtually impossible.[35]

Based on these norms, practical guideline for the information professional can be formulated. Before the formulation of these guidelines, two fundamental aspects must be taken into consideration, namely the recognition of a person's autonomy and freedom as well as the fact that the legal guidelines on privacy do not offer a complete framework for the ethical actions of the information professional with regard to the handling of personal and private information. The concept of autonomy and freedom has already been dealt with. With regard to the juridical guidelines the following comments can be made. Firstly, once a person's private or personal information has been made known publicity (disclaim of the implied intention) .such information is no longer, according to the law, viewed as private This implies that the information can legally be dealt with as trade information. There is therefore (from a juridical perspective) no ethical sensitivity for the autonomy and freedom of the individual with regard to his right to privacy. The second remark relates to the content of legislation itself. As indicated, the immense growth in and development of information technology give rise to the fact that the legislators fall behind in the tabling of appropriate legislation the protection of personal privacy. This is especially true in the South. African situation where there is, for example no legislation on the protection of privacy to provide for information handled via E-mail.[36]

[35] ibid.
[36] ibid.

2. *Public health*

The movement towards interoperable electronic health records will create both new challenges and new opportunities with respect protecting the privacy and security of health information. When protecting Federal information, including personally identifiable information and health information, the Government already has a robust framework in place and numerous policies related to the privacy and security of information, including but not limited to: requirements set forth in the Federal Information Security Management Act (FlSMA), the Privacy Act, office of Management and Budget policies, and guidance and standards put forth by the National Institute of Standards and Technology (NIST). For example, under FlSMA, government information (including health information and personally identifiable information) is required to be categorized and protected based on the level of risk associated with that information. Guidance documents and standards exist for agencies to follow- requiring minimum technical, optional, and management controls.

Health and Human Services (HHS) has promulgated several rules that establish critical foundations of Federal confidentiality, privacy, and security protections for health information across the health care system, including the Health Insurance Portability and Accountability Act 1996 (HIPAA) Private Rule, the HIPAA security rule, and the Confidentiality of Alcohol and Drug Abuse Patient Records Regulation. Taken together, these rules establish the foundational principles of, and from the context for, the comprehensive privacy and security approach HHS continues to take as part of our national health IT agenda. Furthermore, HHS believes the current HIPAA statute provides an appropriate amount of flexibility to protect health information exchanged by HIPAA covered entities in the health IT environment while allowing best practice to emerge. However, there are differences between Federal laws State laws and business practices, which can provide additional challenges for the sharing of health information in a private and secure manner, an issue that is currently being examined.[37]

The number, type, and sophistication of tools that protect electronic information are growing at an ever-increasing rate and provide that opportunity to offer health privacy protections beyond those in the paper environment. For example, implementation of role-based access controls and auditing, when implemented electronically, can limit access to a patient's record to only those individuals who need the information for treatment. Audit trails can automatically record who viewed the health record and can be used after the fact to

[37] Health Insurance Protability and Accountability Act,1996.

identify any unauthorized access, leading, to improvement in training or; if warranted, corrective action.

HHS is very committed to privacy and security as it works toward the President's goal of widespread interoperable electronic health records. Ultimately, the effective coordination of health IT activities will help creates an environment in which the health status of the American public is improved while information remains private and secure.

The HIPAA private rule creates new rights for individuals to have access to their health information and medical records (referred to as "protected health information"), to obtain copies and to request corrections. It also specifies when an individual's authorization is required for disclosure of protected health information; authorization is generally not required for the use of the information and its disclosure for the purpose of treatment, payment or health care operations. The rule applies to health plans, health care providers and health care clearinghouses (which are all "covered Entities"). The vast majority of health care professionals who provide care to adolescents are required to comply.

Under the HIPAA privacy rule, adolescents who legally are adults (aged 18 or older) and emancipated minors can exercise the rights of individuals; specific provisions address the protected health information of adolescents who are younger than 18 and not emancipated Parents (including guardians and person's acting in loco parents) are considered to be the "personal representatives" of their un- emancipated minor children if they have the right to make health care decisions for them. As personal representatives, parents generally have access to their children's protected health information. In specific circumstances, however, parents may not be the personal representatives of their minor children.

A minor is considered "the individual" who can exercise rights under the rule in one of three circumstances. The first situation—and the one that is likely to occur most often is when the minor has the right to consent to health care and has consented, such as when a minor has consented to treatment of an STD under a state minor consent law. The second situation is when the minor may legally receive the care without parental consent and the minor or another individual or a court has consented to the care, such as when a minor has requested and received court approval to have an abortion without parental consent or notification. The third situation is when a parent has assented to an agreement of in each of these circumstances; the parent is not the personal representative of the minor and does not

automatically have the right of access to health information specific to the situation, unless the minor requests that the parent act as the personal representative and have access.[38]

3. *Public Safety*

while gone are the days where Henry Ford would inspect the homes .of workers, employers have new means to acquire information about employees, and these new means require a revaluation of basic fairness in the employee-employer relationship. Many workers are not protected with due process guarantees against arbitrary discharge. Absent state law or contract, employers can often dismiss an employee for any reason, or no reason, even if the decision to terminate is based on false information. At the same time, increased employee monitoring power raise the risk that false inferences can be drawn about employee contact. An employee network-monitoring appliance can detect access to the inappropriate site, but not the intent of the employee. With these new monitoring tools and potential to draw false inferences, it is important now more then ever for employees to have basic due process protections the right of notice of the violation and some "opportunity to be heard". This field is also nuanced. Employees may desire medical screening, including genetic screening, prior to employment.[39]

For instance, in certain workplaces, it is possible to screen an employee for predispositions to disease that may be exacerbated by the presence of chemicals essential to the business. Similarly, background checks are often appropriate for positions of trust, such as a police officer, but not appropriate for jobs unrelated to public safety or the handling of very large sums of money, in the United States and many tired-world countries, workers have very few privacy protections in law. There are few situations where an employee has a due process right to access, inspect, or challenge information collected or held by the employer. There is a patchwork of state and federal laws that grant employees limited rights. For instance, under federal law, private-sector employees cannot be required to submit to a polygraph examination. However, there are no general protections of workplace privacy except where an employer acts tortuously where the employer violates the employee's reasonable expectation of privacy. European employers are bound by comprehensive data protection acts that limit and regulate the collection of personal information on workers. These laws specifically call for purpose and collection limitations, accuracy of data, limits on retention of data, security, and protections against the transfer of data, to countries with weaker

[38] ibid

39)[http//www.newa.cnet.com/2009-1023_272972.HTM, LAST Visited on 15.03.2017]

protections. These protections place employees on an equal footing while allowing employers to monitor for legitimate reason public is going to demand that the government have more ability to conduct surveillance in order to monitor what dangerous people do, "said James Love, director of the Consumer Project on Technology." That is one thing we are going to see happening. But are there ways of dealing with these issues that have any kinds of safeguards built in? What are the realities to prevent the predictable abuses?" Professor Harold J. Krent, of the Illinois Institute of Technology is Chicago-Kent College of Law, takes a longer view. "We have a balance in this society to allow for security and freedom for privacy. That balance changes in such an event," said Krent, who was part of a team that assessed Carnivore. "We are in a new cycle: We'll trade our privacy to be more collectively secure," he added. "We saw this with the Oklahoma bombing and in the columbine shootings, where the government enacted zero-tolerance laws and parental-responsibility laws that both restricted the freedom of some schoolchildren. Well see a similar cycle now.[40]

7.2 CONCLUSION

The digital era has fundamentally transformed the landscape of national security and privacy, presenting complex challenges for democratic societies striving to protect both. This comparative study of the United States, the United Kingdom, and India reveals that while national security legislation is indispensable for addressing threats such as terrorism and cybercrime, it often risks encroaching upon individuals' fundamental right to privacy. Across these jurisdictions, laws have empowered governments with extensive surveillance capabilities, yet frequently lack adequate transparency, judicial oversight, and clear limitations to prevent abuse.

The research highlights common tensions: the need for robust security measures must be balanced with strong legal safeguards that uphold privacy and civil liberties. The U.S., U.K., and India share similar struggles with overbroad state powers and the challenge of adapting existing legal frameworks to fast-evolving technologies. However, the comparative analysis also uncovers valuable lessons—such as the importance of independent oversight bodies, enforceable data protection laws, and constitutional protections that restrict arbitrary surveillance.

[40] ibid

Ultimately, the study underscores the urgent need for reform that embraces a rights-based approach, ensuring that national security efforts are accountable, proportionate, and respectful of privacy rights. Strengthening legal frameworks with clearer limits, transparency mechanisms, and judicial review will help preserve democratic values while effectively addressing security concerns. As digital technologies continue to advance, maintaining this delicate balance will remain a critical task for policymakers, legal practitioners, and civil society alike.

Since the publication of "Right to privacy," courts have struggled to define the scope of civil law-privacy right. Most have agreed that it encompasses the right to benefit from the commercial exploitation of one's name or likeness and to be left alone in seclusion. The difficult question has been the extent to which individuals have a right to keep "private facts" out of the media and unknown to the general public. Because this right conflicts with the rights of free speech and free press, it is particularly troubling for the courts.

While the right to was developing as a civil law concept it also began to appear in cases involving the U.S Constitution. Over tune the U.S. Supreme court decided that common law privacy had a counterpart in the constitution.

The privacy of the individual should receive the added protection of the criminal law, but for this, legislation would be required. Perhaps it would be deemed proper to bring the criminal liability for such publication within.[41]

[41] ibid.

BIBLIOGRAPHY

Books :

1. Beth Givens,The Privacy Right Hand Book,(New York: Avon Books,1997).

Articles :

1. S.M. Masum Billah, 'Right to Privacy: Philosophical Prelude, Development and Challenges.' Mizanur Rahman, Ed.,*HRSS Manual*,(Dhaka: ELCOP,2006).

2. Md.Zahidul Islam and Asma Jahan, 'right to privacy :is it a fundamental rights in Bangladesh constitution?" journal of Asian and African Social Science and Humanities.(2015)

3. Ershadul karim,`Citizen Right To Privacy: Reflection in the International Instruments and Natural Laws',(*Bangladesh Journal of Law, 2005) vol -9 no 1 &2* (2005).

Journal :

1. GLOBAL INFORMATION SOCIETY WATCH, 2014
2. THE Dailystar.

Statutes :

1. The Constitution of the People's Republic of Bangladesh, 1972.

2. The Indian Constitutio,.1947.

3. Health Insurance Protability and Accountability Act, 1996.

4. Technology Information Privacy Code, 2003.

5. The Data Protection Act, 1998.

6. The Privacy Act, 1974.

7. The Universal Declaration of Human Right, 1948.

8. The European Convention on Human Right,1950.

9. ICT Act 2001,2006,2010,and Amendment Act , 2013 of Bangladesh.

10. Privacy International .(2012) BD:Legal Framework.

11. INFORMATION TECHNOLOGY ACT,2000 AND 2008 OF INDIA.

Internet Sources

1. [http://www. Plato stanford.edu/ entrees privacy/last visited on 15.02.2017].

2. [http://www.definitions.uslegal.com/right-to privacy, last visited on 16.02.2017].

3. [http;//www.indiakanoon.org>search>cases, last visited on 20.02.2017].

4. [http://www.en.wikipedia.org/wiki/Privacy, last visited on 10.03.2017].

5. [http://www.rbs2.com/pivacy.htm,, last visited 14.03.2017].

6. [http://www.Privacy international.org/USA/Sur/2003/overview,last visited on 14.03.2017].

7. [http://www.Laws.Justice.gc.ca/en/cha, last visited on 15.03.2017].

8.[http://www.newa.cnet.com/2009-1023_272972.htm,last visited on 15.03.2017]

9. [http://www.Canada Justice.ec.ca /Stable/EN/Laws, last visited on 16.03.2017].

10.[http://www.privacy international.org/report/Bangladesh/ii-legal-framework,last visited on 10.03.2017]