CRIMINAL INVASION OF PRIVACY BY COMMUNICATION THROUGH MOBILE DEVICES:

A COMPARATIVE ANALYSIS OF THE LEGAL REGIMES IN INDIA, UNITED STATES OF AMERICA AND SRI LANKA.

NELSON PRASANNA KUMARANAYAKE

(LL.B.) Attorney-at-Law

LL.M./2019/094

Submitted in partial fulfilment of the requirements for the degree of Master of Laws (LL.M.)

Faculty of Law

University of Colombo

30th September 2021

Declaration

I certify that this extended essay does not incorporate without acknowledgement any material previously submitted for a Degree or Diploma in any University; and to the best of my knowledge and belief, it does not contain any material previously published or written by another person or myself except where due reference is made in the text.

……....

NELSON PRASANNA KUMARANAYAKE

Acknowledgements

I may take this opportunity to thank all those who helped me to make this effort of my extended essay a reality. The research topic is of high importance as at today in the development of technology and extreme use of mobile devices in communication and the risk of invasion by third parties without consent. So that it was really a hard task for me to complete this research if the support of many people was not available at times of need.

I gratefully acknowledge the continuous and valuable support and guidance provided to me by Dr. Thusitha Abeysekara, Legal Studies Unit, Faculty of Management Studies and Commerce, University of Sri Jayewardenepura. I am indebted to Dr. Thusitha Abeysekara for motivational discussions and great support tendered towards me.

My special thanks go to Dr. Dharshana Sumanadasafor his valuable support and guidance given right throughout the LL.M. Programme. It is my pleasure to thank the Dean and the staff of the LL.M./Post Graduate Unit, Faculty of Law, University of Colombo in making me available for the legal resources. I must also take this opportunity to specially thank Dr. Sampath Punchihewa for his cooperation in making corrections and recommendations in my research proposal at first-hand and encouraging me further.

I never forget my beloved wife, Inoka Chandramali and two children, namely; Imasha Kumaranayake and Neron Kumaranayake who tendered their fullest cooperation and helped me in proof reading and correcting where necessary.

List of Abbreviations

ACHR	- American Convention on Human Rights
BASL	- Bar Association of Sri Lanka
CCPA	- California Consumer Privacy Act
CEO	- Chief Executive Officer
CIPA	- California's Invasion of Privacy Act
ECHR	- European Convention on Human Rights
GDPR	- General Data Protection Regulation
GPRS	- General Packet Radio System
GSM	- Global System for Mobile Communication
ICCPR	- International Covenant on Civil and Political Rights
IEEE	- Institute of Electrical and Electronics Engineers
SIM	- Subscriber Information Module
SLR	- Sri Lanka Law Reports
SLCERT	- Sri Lanka Computer Emergency Response Team
UDHR	- Universal Declaration of Human Rights
U.S./USA	- The United States of America
VPN	- Virtual Private Networks
WAP	- Wireless Application Protocol

Abstract

Privacy is a concept in which everyone expects to protect in his or her personal information, data, and private communications from making them public or known to third parties without consent. It is essential for everyone to protect his or her confidential communications from unauthorized and illegal access by third parties. Even the governments indirectly intercept and wiretap such personal communications under the cover of public security provisions contained in the Constitutions, so does in the Constitution of Sri Lanka. There are times when states/government obstruct and block the use of social media communications in times of public disquiet by having resort to the constitutional provisions prevailing at the time, and it clearly violates the people's fundamental freedom of speech and expression of the citizen.

It would be critical when a third party gets illegal access to or invades into the communications that take place through mobile devices, and records them without knowledge of the parties involved in the conversation. This can also happen even by the person who receives a private phone call, gets it recorded without informing the party at the other end which act will violate his or her freedom of expression.

It is yet questionable how to curtail or end such criminal invasions of privacy by communications through mobile devices. For this purpose, it is vital to compare and contrast selected jurisdictions of the United States of America and the Union of India where certain magnificent developments are found in the field under which this research is based.

Keywords

Criminal Invasion

Communication

Data

Decrypt

Encryption

End-to-end encryption

Intercept

Mobile Devices

Privacy

Privacy self-management

Table of Contents

CHAPTER 1

INTRODUCTION

1.1. Background of Research

'It's such an invasion of privacy, you feel like Big Brother's watching you. It baffles my mind. I'm such an open book, you want to know something, you ask.'[1]

Justice Louis Bandeis in the United States Supreme Court argued that while the sanctities of a man's home and the privacies of life are protected by the U. S. Constitution, time works changes, brings into existence new conditions and purposes so that subtler and more far-reaching means of invading privacy have become available to the government.[2] It is the concept of privacy that counts, wrote Brandeis – the "right to be let alone… the most comprehensive of rights and the right valued by civilized men" in Boyd v. United States. [3] This gives green light for discussion in protection of individual privacy form the government.

It is high time that we made certain changes to the laws relating to invasion of privacy in communication, and conversations through mobile devices, for the reason that such conversations may be published or divulged to a third party without the consent of the caller. The invasion of privacy may occur when someone invades into the secrecy of personal

[1] Joseph Cataldo, Quotetab. <https://www.quotetab.com/quotes/by-joseph-cataldo> Accessed 03 March 2021.
[2] Marjorie Heins, 'The Right to be Let Alone: Privacy and Anonymity at the U.S. Supreme (2010) Court' <https://www.cairn.info/revue-francaise-d-etudes-americaines-2010-1-page-54.htm>Accessed 03 March 2021.It was interestingly written that it took thirty-eight years for the Court to overrule it and acknowledge the elementary proposition that electronic surveillance constitutes a search just as surely as a constable's rifling through one's desk or diaries (Katz v. U.S. To this day, the Court and its watchers still struggle over the scope and meaning of Brandeis's "right to be let alone" – when it applies, and what societal or governmental interests are sufficient to overcome it. It is a struggle that becomes more difficult as technology advances to ever more pervasive and sophisticated means of intrusion on private life.
[3] 116 U.S. 616, 630 (1886)

matters and relationships of another. Private and confidential communications are meant to be within the domain of the persons concerned without interference by third or unknown parties even through interception/wiretapping by the government. Most mobile devices such as smart phones and tablet phones nowadays have the facility of recording phone calls whether it be video or voice. The same facility could be used to invade the privacy of another if and when such recordings are used for a purpose other than intended one, without the consent of the party whose voice and image are at issue which would entail criminal liability.

The history of mobile phone communication was explained by Santosh Das (2009) as the Subscriber Information Module (SIM) cards allow use of mobile networks in Global System for Mobile Communication (GSM) which can provide voicemail, faxing, SMS, and high-speed data transfer (WAP). GPRS stands for General Packet Radio System which uses GSM network to transmit data at high speed and used for mobile phone services including internet communication services. In the technology used in mobile phone communication, it is apparent that the use of mobile data or communication go through a network provider which is a government owned or a private company. The question arises whether the private information and calls are recorded and saved in the network provider's data base which again accessible to a third party without the consent of the parties concerned.[4]

It is interesting to note the questions asked by Payton T. M and Claypoole T (2014); Where is the most private place in your life? Your bathroom? Your office? Your car? Your local pharmacy, backyard, or deep in the woods? Can you just disappear for a while and do what

[4] Das Santosh, 'Mobile Phone Communication Technology' (4 June 2009) <http://www.mobilecellphonerepairing.com/mobile-phone-communication-technology.html> accessed 28 May 2021.

you want to do without anyone knowing?[5] The authors nicely submit how society benefits from technology while technological and scientific advances steal your privacy because maintenance of your privacy is important for your freedom to live your life as you like.

1.2. Significance of the Study

Privacy of personal communications must be respected in the society and be protected by the government authorities. Once privacy of an individual is interfered and made available to a third party, it paves the way for many social issues such as blackmails in demanding money, goods or services, family break-ups, and even the loss of life. The prevention from such privacy invasions is essential for a safer and peaceful society. Measures that reduce security of information or that facilitate the misuse of secure information and control system can damage trust which will impede the ability of those technologies to achieve much broader social benefits.[6] The writer in this article further states what James Jefferies, CEO of IEEE quoted that strong encryption of electronic information is an essential tool for assuring the privacy and integrity of our data and systems. IEEE supports the strong encryption to protect the privacy as well as integrity of data and communication.

Privacy is crucial to protect and support many freedoms and responsibilities that we possess in democracy, but unfortunately, our law has reached a point at which the law cannot keep up with the advancement of technology and the constant changes technology brings to our lives.[7] This study shows that the laws should be up to date to tackle with the technological advancements and developments in intruding one's privacy in all respects.

[5] Payton T M and Claypoole T, *Privacy in the Age of Big Data* (Rowman & Littlefield 2014)
[6] IEEE, 'The Importance of Protecting the Privacy and Integrity of Data and Communication' [2018] <https://www.prnewswire.com/news-releases/the-importance-of-protecting-the-privacy-and-integrity-of-data-and-communications-300671266.html> accessed 28 May 2021.
[7] ibid 5

In Sri Lankan perspective, the privacy in general is neither a fundamental right under the terms of the Constitution nor an offence under the Penal Code. However, the Right to Information Act[8] protects certain information which relates to personal information held by the government departments from disclosure under section 5 (1) (a). Although it has been protected and addressed to a certain extent in some legislative enactments passed by the parliament of Sri Lanka, such as; section 07 of the Computer Crimes Act, No. 24 of 2007 and section 53 and 54 of Sri Lanka Telecommunications Act No. 25 of 1991, they do not address the real issue of using private correspondence or communication through mobile devices for a purpose other than the intended one, by a third party, by the sender or receiver of it.

In the article of 'Sri Lanka – Data Protection Overview' (2021), it is stated that presently, Sri Lanka does not have any consolidated and/or specific laws on data protection and the remaining legislation does not provide a definition even for the term 'data'.[9] It is further stated that Sri Lanka does not have any specific legislation on the protection of right to privacy and certain legislative provisions are regarded being relevant use.

Purpose of a phone conversation would be explained in the context whether it be private or commercial in nature, and whether it was made understood to both parties that the conversation may be recorded and used for a different purpose before they start the conversation. There must be a law to deal with such a situation to protect the society at large and individual freedom which would otherwise be at risk in the society. The protection of private communication is mandatory in the society and immediate steps should be taken to

[8] No. 12 of 2016 s. 39. (1) makes it an offence of disclosure of certain information.
[9] One Trust Data Guidance, 'Sri Lanka – Data Protection Overview'(March 2021) <https://www.dataguidance.com/notes/sri-lanka-data-protection-overview> accessed 28 May 2021.

curtail and penalize criminal invasions of such communication in order to end further crimes as well as social issues, such as family break-ups, blackmail of the innocent callers or their families and the increasing cases of suicides.

1.3. Selection of Jurisdictions

The comparative study was done in the jurisdictions of India and the State of California in the United States of America in this research. The relevant jurisdictions have developed the right to privacy to a larger extent, and India possesses the same common law principles which are much more similar to the laws of Sri Lanka. In the State of California in the USA, the data protection and privacy laws have developed with certain landmark judgements. New lessons could be learnt from these two jurisdictions in the field of privacy in communication and its criminality when someone invades into the private domain of another's information or data in communication.

1.4. Limitations

Right to privacy covers a wide area in many respects, so that this research is directed only to the criminal invasion of privacy by communication through mobile devices which are in excessive use by the people around the globe in modern day context. This study of the privacy of communication is restricted to mobile devices with reference to portable tab phones, smart phones, and other types of mobile phones. They are currently used as the main stream and common mode of communication by individuals all over the world. The hand-held devices are considered as an essential item specially among the youth.

The privacy laws and their development are comparatively considered and analysed with respect to India, State of California in the United States of America and Sri Lanka. Several legislative enactments, journal articles, websites, and decided case laws are referred to and considered, from which new knowledge can be obtained. The study of legal framework in the selected jurisdictions directly facilitates for necessary recommendations and amendments in developing legal system of Sri Lanka.

1.5. Chapter Outline

In this work, careful analysis of the legal background is done in order to see whether recommendations for the protection of privacy on individuals are possible to be made out.

Various chapters are included in this work as described below:

Chapter 1 mainly deals with the introduction of research background, significance of the study, selection of jurisdictions, and limitations, and limitations. In chapter 2, the research focuses on the methodology, with sub topis of research problem, research questions, hypothesis, objectives of the research, definition of key words, collection of primary and secondary data, data collection system, and methods of data analysis.

The chapter 3 basically analyses literature review in this research paper with an introduction of various articles, judgements, web blogs in the selected jurisdiction of Sri Lanka, India, and United States of America. In chapter 4, discussion and analysis of the legal systems with defining what the criminal invasion of privacy in communication means, applicable legal framework for the protection of privacy in communication, existing legal framework in Sri Lanka with the constitutional and penal provisions including various legislations.

In chapter 5, the research is directed to discuss about findings and possible recommendations in the protection of privacy and the chapter 6 is limited to the conclusion with executive summary of the research and further research.

This paper articulates the present scenario of India, United States of America, and Sri Lanka for the protection of individual privacy in the criminal justice system and how to curtail the invasion of one's privacy in communication manly through mobile devices.

CHAPTER 2

RESEARCH METHODOLOGY

2.1. Research

2.1.1. Research Problem

Inadequacy of protection in the existing legal regime in Sri Lanka for individual privacy in communication through mobile lets criminals free to invade into one's domain of private and sensitive information through various applications, call recorders, smart phone cams, and tablet phone cameras. Recording voice calls and video calls without the consent of caller or receiver. Most of the crimes of this nature in privacy violations are rarely reported to the relevant authorities because he or she is reluctant in divulging such acts concerning the privacy of the victim. Even in the reported cases, it is be impossible for the victims to meet justice due to suppression of material facts by themselves. Criminal invasion of privacy may result in family breakups, loss of life, socio-economic problems, secondary victimization in the society, and also increase of crime rate.

In Sri Lanka, there are no clear legal enactments for the absolute protection against the violation of privacy and victimization of individuals in communication through mobile devices. In order to combat violations of privacy, imposition of civil liability may result in a long-dragged procedure to bring the wrongdoer before justice, and have relief. The need has arisen to impose expeditious remedy in banning such illegal activities and curtail further victimization by the imposition of criminal liability. It is, therefore, essential to reconsider whether any recommendations can be made to fill this lacuna, whereas penalising acts of criminal invasion of privacy becomes mandatory by supplementing amendments to the Penal Code.

2.1.2. Research Questions

1. What is the definition of criminal invasion of privacy in the context of information and communication technology?
2. What is the applicable legal framework for protection of privacy in communications through mobile devices in Sri Lanka?
3. Does the current legal framework in Sri Lanka provide adequate protection to deal with the situation?
4. What lessons can we learn from the selected jurisdictions in India and United States of America for the protection of privacy in communication?
5. What recommendations and amendments can be introduced to reform the law relating to privacy by communication through mobile devices?

2.1.3. Hypothesis

Imposition of criminal liability and penal sanctions will facilitate to protect the privacy in communication through mobile devices and minimize the crime rate.

2.1.4. Objectives

- To define criminal invasion of privacy in the context of information and communication technology,
- To analyze the applicable legal framework for the protection of privacy in communication by mobile devices in Sri Lanka,
- To ascertain whether the legal framework in Sri Lanka is adequate to deal with the situation,
- To compare and contrast the legal regimes in the selected jurisdictions of India and California in the USA,

- To make recommendations and amendments to reform the existing laws in Sri Lanka in order to protect privacy in communication.

2.1.5. Definition of key words and terms

Privacy - right to be let alone.[10]

Mobile device - A portable device such as a mobile phone or a smart phone or a tablet computer which you can use in different places.[11]

Intercept calls - Tap a telephone or telegraph wire to get information.[12]

Encryption - Process of converting electronic information into a secret code that hides information's true meaning.[13]

End-to-end encryption - Messages sent to one device that only can decrypt it and messages travel all the way from the sender to the recipient in encrypted form.[14]

Communication - Importing or exchanging information by speaking, texting or using some other medium.

Criminal Invasion - An unwelcome intrusion into another's domain without consent or knowledge of the other.

2.2. Primary and Secondary Data

2.2.1. Primary Data

Primary data is mainly collected through a number of legislative enactments and case reports available in the field in Sri Lanka and other selected jurisdictions.

[10] Samuel D Warren and Louis D Brandeis, *The Right to Privacy* Vol. IV (Harvard Law Review Association 1890)
[11] Cambridge Dictionary. <https://dictionary.cambridge.org/> Accessed 01 July 2021.
[12] Definitions. <https://www.definitions.net/definition/intercept> Accessed 01 July 2021.
[13] Peter Loshin, 'encrption' <https://searchsecurity.techtarget.com/definition/encryption> Accessed 26 June 2021
[14] Kaspersky Team, 'What end-to-end encryption is, and why you need it' (2020) <https://usa.kaspersky.com/blog/what-is-end-to-end-encryption/23288/> Accessed 26 June 2021

The primary data is mainly analysed in the Constitutions of Sri Lanka and the other selected jurisdictions, while the penal codes and evidence ordinances as well as the other acts are referred. There are several legislative enactments that were passed by the parliament of Sri Lanka for the protection of data in telephone calls, as in the Computer Crimes Act No 24 of 2007, Electronic Transactions Act No 19 of 2006, and Telecommunications Act No 25 of 1991. The Supreme Courts of Sri Lanka, India and Unites States of America held the privacy in communication through telephone calls to be protected which aided in analysing for this study in communication and privacy. Several International Covenants were also helpful as means of primary data collection.

2.2.2. Secondary Data

Secondary data is collected from earlier researches and works done by local and international scholars in the same field through journals, books, websites and blogs. There is a fantastic collection of rich articles on the data protection and call recordings in India as well as in the U.S. that helped to learn lessons and progress further in this study.

2.2.3. Qualitative and Quantitative Data

This research is based on modern day context in digital world on the use of mobile smart phones and devices to record phone calls and tapping by the governments or a third parties. This study is conducted by analysing both local and international material qualitatively. Journal articles of many scholars in the field were discussed in order to find whether reasonable protection is offered or suggested against criminal invasion of privacy.

2.2.4. Data Collections System

The data was collected through online research in the field of privacy of communication. The use of internet and google search were much helpful. Primary sources were collected from legislations and judgements while secondary sources were referred from books, dictionaries, journal articles, websites and blogs.

Library research was done in my own chambers and with remote access to other library based website in the University of Colombo. Decided case laws by the Supreme Court of Sri Lanka were found in the BASL law journals and the supreme court website as well. Two main jurisdictions were selected in India and the USA, while comparison was done with Sri Lanka, because there have been significant developments in the field of privacy laws there. Practical and theoretical ideas of earlier researches were very important in the same field in finding what is left with no answers.

2.2.5. Methods of Data Analysis

Collected data from primary and secondary sources in the legislative enactments, journal articles, and available judgements, was analysed through careful observation in order to find out whether they cover the protection against criminal invasion of privacy of communication. The suggestions and observations of the early researchers in the field of data protection were considered to decide necessary recommendations.

Comparative legal study was made with reference to theoretical ideas published in the legal regimes of India and United States of America with Sri Lanka, to see how technological developments are used in protecting individual privacy against invasion and decide on further recommendations to enact new laws into the legal system of Sri Lanka.

CHAPTER 3

LITERATURE REVIEW

3.1. Introduction

The literature review in this study deals with scholarly articles, legislative enactments and other published material in the field of privacy and communication having special focus on the Sri Lankan legal system. Various journal articles and case laws were referred to in Sri Lanka, in India and in the U.S. to see what protection is available for individual privacy of communication whether it be a fundamental right in the Constitutions or an authority in the decided case laws.

The World Bank submits a report in 2002 on electronic security and the need for more effective electronic security may sometimes conflict with and negatively affect the user's privacy. Inadvertently, it may also affect the privacy of third parties who are identified in affected information.[15] It is the privacy which is an issue of fundamental importance, reflecting the very substance of our cultural identities, values, and more. It should be handled with utmost care, which is a good example of how privacy is described.

Universal Declaration of Human Right (UDHR) was the first attempt to formulate a right to privacy as a separate fundamental right and International Covenant on Civil and Political Rights Act (ICCPR) is based on it, protects 'privacy', 'family', 'home', and 'correspondence' from 'arbitrary' or 'unlawful' interference.[16] European Convention for the Protection of Human Rights and Fundamental Freedom and American Convention on Human Rights

[15] Glaessner T, Kellermann T, McNevin V. (June 2002) 'Electronic Security: Risk Mitigation In Financial Transactions Public Policy Issues' (2002) The World Bank <https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.119.8602&rep=rep1&type=pdf> Accessed 23 July 2021.

[16] Sooriyabandara V. 'Balancing the Conflict between Right to Information and Right to Privacy under Sri Lankan Fundamental Rights Perspective' (2016) Sabaragauwa University Journel.

(ACHR) prefer the term ***'private life'*** to ***'privacy'***, while the former also substitutes ***'family life'*** for ***'family'***.[17]

Privacy principles embodied in Canada's federal regime includes information collected, shared and used for specific purposes, data stored and disposed of responsibly, people's right to see information gathered about them, and people's right to complain if personal data is used for unintended purposes[18]. This refers what governments should do in order to protect the privacy of the citizen when ruling a country and not invading privacy on the national security clauses.

3.1.1. Sri Lanka

Sri Lanka has no clear and enforceable provisions for the protection of one's privacy in communication through mobile devices, although some guarantee is provided for the protection of interception and wiretapping by the acts passed in the parliament. Protection of privacy in communication directly links with the data as it is used to generate internet and social media calls through various applications downloaded in the mobile devices.

Data Protection Laws

Carefully drafted data protection laws are necessary for the protection of privacy in communications through mobile devices, due to the extensive use of mobile data and wi-fi in chats, voice or video calls, and sharing information around the globe. It is unsafe to use data without proper knowledge where any device can remotely be accessed by a third party through various applications and google platforms. Data protection laws should have a parallel safeguard on the rapid development of technology and maintain a balance.

[17] Sooriyabandara V. (December 2016) 'Balancing the Conflict between Right to Information and Right to Privacy under Sri Lankan Fundamental Rights Perspective' Sabaragauwa University Journel. p. 4
[18] Jim Bnskill and David McKie, *Your Right to Privacy* (International Self-Counsel Press Ltd.2016)

The European Union initiated “Data Protection Directive 95/46/ec” and all member countries implemented domestic laws to supplement the General Data Protection Regulation (GDPR) which requires the consent of subjects for data processing, anonymizing collected data, and providing data breach notifications[19] According to the writer, personal data protection in Sri Lanka has been a non-existent concept and is currently dictated by ad hoc rules that may be found in other statutes or licenses and regulations and the proposed data protection act is more or less a replication of the GDPR save some minor changes.

Delict v Crime

According to an article published in 2021; Chapter II of the Constitution of Sri Lanka 1978 does not guarantee a right to privacy as a fundamental right and the right to privacy is protected as a 'delict' within the notion of *actio iniuriarum* and has been developed by case law.[20] In *Nadarajah v Obeysekera*[21], the notion of 'invasion of privacy' was discussed. It was recognized that the right of individuals to personal space exists. In more recent cases related to individual privacy in *Hewamanna v Attorney General*[22] *(1999)* and *Sinha Ranatunga v. State*,[23] the Supreme Court of Sri Lanka highlighted the importance of the individual's right to privacy. In this article, it is stated that the provisions of Electronic Transactions Act No. 19 of 2006 deal with the protection of communications in the commercial nature transactions, and section 2. 3 is applicable to any data or communication made via electronic form, while Computer Crimes Act No. 24 of 2007 regulates cases where data has been unlawfully obtained, intercepted, and disclosed, but does not specifically provide or define what ‘data’

[19] Janith Wijekoon ‘Feature Story 2: Recent Developments in Data Protection Laws in the World and Personal Data Protection Law in Sri Lanka’ <https://www.juniorbarbasl.lk/assets/files/Feature%20Article%202.pdf> Accessed 03 August 2021.
[20] OneTrust Data Guidance, ‘Sri Lanka – Data Protection Overview’ (March 2021) <https://www.dataguidance.com/notes/sri-lanka-data-protection-overview> accessed 29 May 2021.
[21] 52 NLR 76 (1971)
[22] ‘EPIC – Privacy and Human Rights Report’ (2006) <http://www.worldlii.org/int/journals/EPICPrivHR/2006/PHR2006-Republic-28.html> Accessed 20 June 2021.
[23] 2001 (2) SLR 172

is. Section 2 of the Computer Crimes Act provides that the Act is applicable to computers and information contained in computers. It states about the 1978 Constitution of Sri Lanka as it does not guarantee the right to privacy as a fundamental right although Article 14 A mentions privacy considerations within the context of restrictions to the right of access to information as provided by law. The restrictions on the exercise of this right are placed in the interests of national security, territorial integrity and public security. It is confirmed in the said article that Sri Lanka does not have any specific regulation on the protection of privacy.

However, these provisions do not guarantee the protection of privacy in communication by express wording in any legislative enactments passed by the parliament. Even the supreme law in the country, the Constitution of 1978 does not provide protection on the right to privacy or consider it as a fundamental right of the citizen. The right to privacy is an inherent right in the freedom of speech and expression including publication which is protected in the Article 14 (1) (a) of the Sri Lankan Constitution, nevertheless, right to privacy in personal conversations and communications are not included. The restriction in Article 15 (7) is that this right of freedom of speech, expression, and publication is subject to such restrictions as may be necessary in the interests of national security, public order, and the protection of public health or morality, or for the purpose of securing the recognition and respect for the rights and freedoms of others. This protects privacy of people by limiting the publication of every information. Public morality is linked with privacy of the people, however, the concept of privacy is not expressly included in Article 15 (7), so that it is open for invasion in Sri Lanka. Right to privacy should be a basic right of every citizen and be protected against illegal and criminal invasion by anyone whether it is a public body or a private person. If the right to privacy is included as a fundamental right, the protection of personal communications may well be balanced.

The above article focuses on a draft bill for the protection of data and privacy which is essential in a time of digital revolution taking place and abuse of communications is open. The judgements cited in the above article do not guarantee any privacy rights by communication through mobile devices and private audio or video calls. Several Acts of parliament are referred in the same study for the protection of information and data, although they do not protect privacy rights of the people's communication.

Technology v. Legal Reform

Marsoof[24] in his study of 'Privacy at stake! Technology v. Legal Reform' emphasizes the need for privacy protection as a fundamental right because it is a fundamental right in many countries. It is a clear and acceptable point of view taken by the author that Sri Lankan and Indian Constitutions do not expressly guarantee the right to privacy. The author cites privacy in four aspects; information, bodily, communication, and territorial in which data protection is an aspect of privacy. He discusses that in public switch telecommunications networks, grid of cables that connect every point in the network through portals known as 'Gateways' provide great opportunity for information theft which is commonly known as "Telephone-Tapping".

Justice Kuldip Singh of the Indian Supreme Court in ***People's Union of Civil Liberties v Union of India AIR***,[25] declared that Telephone-Tapping is a serious invasion of an individual's privacy and within the growth of highly sophisticated communication technology, the right to hold telephone conversation, in the privacy of one's home or office without interference is increasingly susceptible to abuse.

[24] Bar Association Law Journal (2009) Vol XV p 75
[25] AIR 1997 (SC) 568.

The author goes onto discuss the Telecommunications Act No 25 of 1991 as the only legislation that provides for some protection and its applicability to the protection of data and regulating the interception of telecommunication transmissions, and the disclosure of their contents has been made an offence subject to penalty and imprisonment under sections 53 and 54 (1). This protection of personal communications through telephones does not protect the disclosure of any information by the caller or receiver who recorded the same through any form of mobile device, but only interception of telecommunications. This Act was amended by Act No 27 of 1996 without any additions or changes made to those penal sections which could be used as an ad hoc remedy in the protection of individual privacy.

Budapest Cyber-crime Convention

Fernando[26] in his study on 'Budapest Cyber-Crime Convention and its impact on the Sri Lanka ICT Legal Regime' expresses that Sri Lanka became a state party to the Council of European Convention on Cyber Crime (Budapest Convention). According to the author, it is the only international treaty on internet and computer crime that seeks to harmonize national laws, adopts improved investigative powers based on international standards, enhances criminal justice cooperation among State Parties in order to effectively combat the threat against cybercrime. Sri Lanka, being a dualist country, needs to enact laws in the parliament to take the convention into effect and legally binding. The writer comments that the Computer Crimes Act No 24 of 2007 was modelled on Budapest Convention to harmonize legislation with the Convention. This convention basically deals with the subject of cybercrimes which are classified as offences against the confidentiality, integrity and availability of computer data and systems, which include offences such as illegal access, illegal interception, data interference, system interference and misuse of devices.

[26] Bar Association Law Journal (2016) Vol XXII p 277

It is clear that offences must be committed internationally for criminal liability to arise, so that locally committed offences are not enforceable under the Convention. Budapest Cybercrime Convention is a criminal justice convention and, therefore, it is a criminal justice response to cybercrime offences. Some concerns have been raised whether "warrantless wiretapping" would be legitimized or enhanced because of the interception provisions contained in section 18 of the Act.

A close review of the Computer Crimes Act of Sri Lanka would show that it is the exception rather than the rule. Under the provisions of Computer Crimes Act, a Magistrate's Court order is a *'sine quo non'* for such interceptions. Warrantless wiretaps (Interceptions) in most countries take place under national security provisions by gaining access to telecommunication systems using security related regulatory regimes.

In this article, the writer does not discuss of individual privacy in protection of mobile/wi-fi data and call recordings being misused by caller or receiver or the State. The privacy concerns are considered here on cybercrimes via computers internationally, however, it is not a strange thing that privacy in internet communication takes place as same as data communication over mobile phones in voice or video calls.

It is very important to enact laws to the effect that warrantless wiretapping should not take place in the personal one-to-one confidential telephone conversations even in the situations under national security. The governments take use of national security cover in the Constitutions in order to curtail or limit the social media communications and indirectly intercept private calls any reasonable cause.

Computer and Internet Crimes

Abeynayake,[27] in his work of 'Applicability of Information Technology Law to avoid Computer and Internet Crimes in Sri Lanka" states that the Sri Lanka Computer Emergency Response Team (SLCERT) is the centre for cyber and internet security in Sri Lanka, permitted to protect nation's information infrastructure and to coordinate protective measures against the responses to cyber security threats and vulnerabilities. Relevant legislation in the IT law in Sri Lanka is Electronic Transactions Act No. 19 of 2004, Computer Crimes Act No. 24 of 2007, Payment Devices Fraud Act No. 30 of 2006 and Penal Code (Amendment) Act No. 16 of 2006. These legal enactments mainly deal with offences relating to computer crimes and use of computer services for sexual abuse of children. The author speaks of individual privacy and data protection by emphasizing that the legal systems should be developed to penalize hackers and those who invade into the personal and confidential information of individuals. Punishing those who invade into one's privacy in communication would affect in reducing such illegal acts.

In the landmark case of *Hewamanne v. De Silva and another*,[28] the Supreme Court of Sri Lanka decided, among other things, that the law of contempt of court will continue to operate untrammelled by the fundamental right of speech and expression. Honourable Justice Wanasundara expressed with approval *that "Although the Constitution does not specifically refer to the press, the provisions guaranteeing the Fundamental Right of speech and expression to every citizen are adequate to ensure the freedom of press in this country"*[29]. This expression has a weight in this discussion to interpret the Constitutional provisions in Sri Lanka in order to see what is not guaranteed.

[27] BALR (2011) Vol XVII p 138
[28] (1983) 1 SLR 1
[29] ibid 28 p. 4

Although the right to privacy is not expressly included in the Constitution of Sri Lanka, it is included in the Fundamental Rights Chapter in Article 14 (1) (a), read with and subject to restrictions laid down in Article 15 (7).

It is significant to consider the Sri Lankan Court of Appeal judgement of *Sinha Ranatunga v. The State*[30] at this point. Publication of defamatory statements in the press and they may be defamatory even though the readers do not believe it to be true, and the meaning intended by the writer or the publisher may not be very relevant. So, publication of statements attracts liability and does matter what is intended by the person who does the act. This should be made a strict liability offence (acts attract liability without intention) in the Penal Code. This judgement was delivered in the year 2000 before the amending Act No. 12 of 2002 in the Penal Code which repealed the chapter relevant to defamation as a crime. It was held that the Penal Code makes the requisite criminal intention or knowledge as an additional ingredient of the offence of defamation. The same chapter should be restored and made it a strict liability offence without considering the intention or knowledge of the person who makes the statement or publication of phone conversations.

In the Court of Appeal, Honourable Justice Yapa elaborated the fact that the press should not think they are free to invade the privacy of individuals in the exercise of the constitutional right to freedom of speech and expression merely because the right to privacy is not declared a fundamental right of the individual, and the law of defamation both civil and criminal is also geared to uphold the human beings right to human dignity by placing controls on the freedom of speech and expression.[31]

[30] (2001) 2 SLR 172
[31] ibid 30

This makes sense for new thinking that privacy rights of the people are of utmost importance in the current society and should be protected. The restrictions must not be made on fundamental rights of the people as done in the Article 15 (7). Another important point was raised by Justice Yapa as follows;

"In this instance it is usually irresponsible conduct on the part of the press misusing its freedom of speech and expressions to injure another's reputation or indulge in what is called, character assassination."[32] This is open for discussion in connection with the preserving of the right to privacy in individual communication.

3.1.2. India

The right to privacy is not expressly provided under the Constitution of India, however, implicitly takes into it the right to privacy as personal liberty guaranteed under Article 21 of the Constitution.[33] The right to privacy is recognized by the Supreme Court of India recently by a nine-judge bench in the case of *Puttuswamy v. Union of India*,[34] declaring that the right to privacy is a fundamental right protected under Part III of the Constitution of India.

In India, section 72A of the Information Technology Act applies to any person who, while providing services under the terms of a lawful contract, has secured access to any material containing personal information about another person. And penal sanction is imposed on such person if he discloses such material without the consent of the person concerned or with intent to cause wrongful gain or loss.[35]

[32] 2001 (2) SLR 175
[33] Shiv Shankar Singh, (2011) 'Privacy and Data Protection in India: A Critical Assessment' Vol. 53. Indian Law Institute <https://www.jstor.org/stable/45148583> Accessed 03 August 2021.
[34] (2017) 10 SCC 1
[35] Rohas Nagpal, *Data Privacy Law (India)* (Asian School of Cyber Laws 2012)

Negpal R. further discusses in his study on the privacy policy for handling of or dealing in personal information including sensitive data or information which should manifestly include telephone call recordings, tapping and data protection, if the recording takes place without the consent of the party concerned in providing services under a lawful contract rather it does not focus on personal correspondence of an individuals in daily life.[36] The Information Technology Act provides protection of privacy rights of individuals, nevertheless, communications and sensitive data transferred through wireless mode in phone calls has to be covered further.

Phone Tapping and Recordings of Telephonic Conversations

Dalmia[37] in his research article of 'Phone Tapping and Recording of Telephonic Conversation - Right to Privacy and Indian Law' expresses certain views on privacy of individual communication as a right, and not as a crime in order to protect the individual damage caused by its publication or giving access to a third party without consent. Article 21 of Constitution of India enacts *"No person shall be deprived of his life or personal liberty except according to procedure established by law"*.

In a plethora of judgments 'Right to Privacy' has been held as an integral part of the 'Right to Life' and 'Personal Liberty' enshrined under Article 21 of the Constitution.[38] In the case of *R.M. Malkani v. State of Maharashtra*[39] the Supreme Court observed "*The telephonic conversation of an innocent citizen will be protected by Courts against wrongful or high handed interference by tapping the conversation. Protection is not for the guilty citizen…."*

[36] Rohas Nagpal, *Data Privacy Law (India)* (Asian School of Cyber Laws 2012)
[37] Vijay Pal Dalmia 'Phone Tapping and Recording of Telephonic Conversation- Right to Privacy and Indian Law' [2018] <https://www.mondaq.com/india/Privacy/707096/Phone-Tapping-And-Recording-Of-Telephonic-Conversations-Right-To-Privacy-And-Indian-Law> accessed 03 March 2020
[38] ibid 37
[39] 1973 AIR 157

The author father goes onto state that from above case laws, it is amply clear that 'Right to Privacy' includes right to hold telephonic conversation without any interference. The act of recording by any person (being the sender or recipient of the information) of a telephone call which originates from or ends at his telephone cannot be construed as an 'interception' within the meaning of the Indian Telegraph Act, since a recorded conversation to fall within the ambit of 'interception' the content of the information is to be made available to a person other than the sender and the recipient or intended recipient of that communication.[40] However, the writer does not focus on the protection of privacy in criminal invasion of individual communication and how to curtail, but deals with right to privacy.

In the same case of *R.M. Malkani v. State of Maharashtra,*[41] it was decided that where a person talking on the telephone allows another person to record it or to hear it, it cannot be said that the other person who is allowed to do so is damaging, removing or tampering for intercepting with the contents of any message. This emphasizes when and how criminal liability on invasion of privacy to be imposed. The exceptions have to be provided when parties consent for call recordings. Supreme Court further held that the telephonic conversation of an innocent citizen will be protected by Courts against wrongful or high-handed interference by tapping the conversation.

In *Rayala M. Bhuvaneswari vs. Nagaphanender*[42] *Rayala* High Court of Andra Pradesh held that the act of tapping itself by the husband of the conversation of his wife with others was illegal and it infringed the right of privacy of the wife.

[40] Vijay Pal Dalmia 'Phone Tapping and Recording of Telephonic Conversation- Right to Privacy and Indian Law' [2018] <https://www.mondaq.com/india/Privacy/707096/Phone-Tapping-And-Recording-Of-Telephonic-Conversations-Right-To-Privacy-And-Indian-Law> accessed 03 March 2020
[41] 1973 AIR 157
[42] AIR 2008 AP 98

Interception of messages is allowed under the section 5 of the Indian Telegraphs Act. According to the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 defines "intercept" as any information through the use of means, including an interception device, so far as to make some or all of the contents of information available to a person other than the sender or recipient or intended recipient of that communication and includes-

a) Monitoring of such information,

b) Viewing, examination or inspection of the contents of any direct or indirect information and

c) Diversion of any direct or indirect information from its intended destination to any other destination.[43]

This is a new aspect of call diversion or forwarding, although it does not include conference calls that are made without the consent or knowledge of the parties involved. the writer further states the act of recording by any person of a telephone call which originates from or ends at his telephone cannot be construed as 'interception' within the meaning of the Indian Telegraph Act, since a recorded conversation to fall within the ambit of 'interception' the content of the information is to be made available to a person other than the sender and the recipient or intended recipient of that communication. The writer does not talk about how the recordings can be made available legally to prove or disprove a case of privacy violation.

[43] Vijay Pal Dalmia 'Phone Tapping and Recording of Telephonic Conversation- Right to Privacy and Indian Law' [2018] <https://www.mondaq.com/india/Privacy/707096/Phone-Tapping-And-Recording-Of-Telephonic-Conversations-Right-To-Privacy-And-Indian-Law> accessed 03 March 2020

The report of 'Privacy and Data Protection Aspects in Indian Cyber Space' says Privacy Protection requirements are important for both Individuals and Organizations alike. There have been many attempts in India to formulate a dedicated Privacy Protection Law but failed so far.[44] This again raises the doubt whether privacy protection laws are sufficient in India to curtail criminal invasion of privacy.

Privacy and legal protection

Geetika Rustagi (2014) talks on privacy concerns of celebrities when they are hacked and says that Indian law does not determine what privacy is, but only the situations where privacy will be afforded legal protection. The author equates privacy with confidentiality and explains how some photographs were published in hacking their computers. It is explained that India also existed privacy under tort law until Information Technology Rules in 2011 came in, to protect privacy of individuals and their personal information. In that sensitive personal information is analysed only the password, financial information, physical health conditions, sexual orientation, medical records, and biometric information. This does not cover very important personal conversations over the telephone and call recordings done without the consent of the caller or receiver.

The Court of Last Resort in India (Supreme Court) reached the conclusion that right to privacy as a fundamental right that is generated by Part III of the Indian Constitution on 24th August 2017[45].

[44] Global ICT Policies And Strategies And Indian Perspective by Global ICT Policy Formulation, Implementation and Its Performance Analysis <http://ptlb.in/iips/?p=405> accessed 03 March.2020.
[45] Rishabh, 'A Critical Analysis on Data Protection and Privacy Issues in India' Legal Service India E Journal. <https://www.legalserviceindia.com/legal/article-2705-a-critical-analysis-on-data-protection-and-privacy-issues-in-india.html> Accessed 03 March 2021.

This approach should be developed in every country when interpreting the Constitutional provisions on the right to privacy in fundamental rights chapters. The article goes on to mention that India does not have any comprehensive legislation in the protection of data and privacy, as in Sri Lankan. Article 21 of the Indian Constitution mandates that no individual will be in hardship of his/her own freedom or life.

Data Protection in India

In *Justice K. S. Puttaswamy (Retd) vs. Union of India*[46], the Supreme Court of India held Aadhaar (Unique Identity) is a serious invasion into the right to privacy of persons and has the tendency to lead to a surveillance state where each individual can be kept under surveillance by creating his/her life profile and movement.

Justice Nariman, in his separate opinion held; *"The judgement Puttaswamy recognizes the right to privacy is a constitutional guarantee protected as intrinsic to the freedoms guaranteed by Part III of the Constitution"*[47]

Janith Wijekoon mentions that this judgement reiterates the need for a comprehensive data protection regime to achieve the same objective, and in Sri Lanka, the need of laws to protect personal information that is being stored electronically.[48] This calls for question why the necessary actions are not taken to protect data and privacy by implementing necessary legislative enactments and legal authorities to monitor the privacy violations.

[46] Writ Petition (Civil) No. 494 of 2012 decided on 24 August 2017.
[47] ibid 46
[48] Janith Wijekoon, 'Feature Story 2; Recent Developments in Data Protection Laws in the World and Personal Data Protection Law in Sri Lanka' <https://www.juniorbarbasl.lk/assets/files/Feature%20Article%202.pdf> Accessed 03 August 2021.

3.1.3. The United States of America

Privacy concerns are critical in America as it is open to be misused by criminals**.** Americans express a consistent lack of confidence about the security of everyday communication channels and the organizations that control them, particularly in online use of tools public or private, in protecting the personal information they collect[49]. In this work, it was revealed that younger adults are more likely to know that personal information about them is available online, and to have experienced privacy problems. It is also suggested that a majority of the U.S. public believes changes in law could make a difference in protecting privacy. This is a good tendency towards privacy protection and the enforceable penal laws against criminal invasion of individual privacy will facilitate to protect the privacy of individual.

It was submitted by Tajdar Jawaid that individuals are not comfortable to share very innocent, totally harmless personal information with anyone, and privacy is a state of not being watched or disturbed without our knowledge and consent.[50] In United States, the fourth amendment[51] considered to be basis of most privacy laws, and multiple federal and state specific laws were enacted to ensure the privacy rights of an individual. According to this article, it is clear the governments should take steps to ensure the privacy of individual by enacting laws and implementing them without bias.

It was further stated by Tajdar Jawaid what privacy related data is, and technically anything considered to be private related to personal data which a person is not willing to share with

[49] Pew Research Center 'The State of Privacy in Snowden America' [21 September 2018] <https://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/> Accessed 03 August 2021.

[50] Tajdar J, 'Privacy Vs. National Security' (July 2020) <https://arxiv.org/ftp/arxiv/papers/2007/2007.12633.pdf> Accessed 03 August 2021.

[51] ibid 50. p. 2. "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"

the world. The writer cites European General Data Protection Regulation (GDPR) of 2016 in which personal data is meant any information about a natural person (living person).[52]

Governmental power to protect the privacy of its citizens by penalizing publication and privacy as a concept composed of several aspects; protection from unreasonable intrusion upon one's seclusion, from appropriation of one's name or likeness, from unreasonable publicity given to one's private life, and from unreasonable publicity placing one in a false light before the public.[53] This article continues that court has variously recognized valid governmental interests in extending protection to privacy, it has nevertheless interposed substantial free expression interests in the balance.[54]

Accordingly, the freedom of expression and protection of privacy should be balanced in the interpretation of legislature by the judiciary as done for years in every country. The invasion of privacy attracts civil liability in America and it needs to be penalized as a criminal activity for intrusion of privacy without permission.

Data Protection in the USA

USA lacks a central data protection authority and federal enforcements have taken place in certain States to protect personal data, such as California Consumer Privacy Act (CCPA) which provides certain privacy rights to individuals and enables individuals to bring private actions against any violations of certain unencrypted personal information.[55] It is surprising

[52] Tajdar J, 'Privacy Vs. National Security' (July 2020) <https://arxiv.org/ftp/arxiv/papers/2007/2007.12633.pdf> Accessed 03 August 2021.
[53] Legal Information Institute 'Invasion of Privacy' <https://www.law.cornell.edu/constitution-conan/amendment-1/invasion-of-privacy> Accessed 03 August 2021.
[54] ibid 53
[55] Janith Wijekoon, 'Feature Story 2: Recent Developments in Data Protection Laws in the World and Personal Data Protection Law in Sri Lanka' <https://www.juniorbarbasl.lk/assets/files/Feature%20Article%202.pdf> Accessed 03 August 2021.

that the USA with extreme use of data in many fields including the defense of the government, has not a data protection authority in force. A data protection authority which is independent from other organs of the government needs to be implemented to secure the privacy of individual.

In the United States, the Privacy Act governs the collection and use of personal information in the federal government sphere, while the Federal Trade Commission polices the abuse of private data affecting consumers.[56] It was further stated that revelations about widespread surveillance of online communications reverberated in recent years, sparking an international convention on digital privacy.

This amply shows that the need of protecting the data and online communications is of high demand at present. The author further speaks of international agreements that 99 countries have enacted privacy laws. The communication via mobile devices should be protected and privacy legislations are required to monitor them in technology developments.

Call Recording in California

Mark E. Ells expresses his ideas in California legal regime and ideas on California's Invasion of Privacy Act (CIPA), found at Penal Code section 630 which was enacted to protect the right of privacy of the people and with the advent of new devices and technology, and use of them has created a serious threat to the free exercise of personal liabilities. CIPA makes it illegal; wiretap by section 631, and record telephonic communications by section 632 or

[56] Jim Bnskill and David McKie, *Your Right to Privacy* (International Self-Counsel Press Ltd.2016)

record without consent cell phone communications by section 632.7.[57] Penal Code of California section 632 (c) excludes communications made in which the parties may have reasonable expectation that it may be overheard or recorded. This can be taken as a recommendation to include in the Sri Lankan legal regime in order to curtail criminal invasion of privacy in communication.

This gives strength for new thinking to enact laws and penalize those who record telephone calls without consent and use it in violating the privacy in communication. It is an interesting approach when California legislature declared that with the advent of new devices and technology used for the purpose of eavesdropping upon private communications, the resulting invasion of privacy from the use of such devices and techniques has created a serious threat to the free exercise of personal liabilities and cannot be tolerated in a free and a civilized society. The CIPA prohibits various forms of international recording and eavesdropping without consent so that it protects confidential communications. Several case laws were cited by the author in the article, where a distinction is drawn between monitored calls and recorded calls.

3.1.4. International Conventions

International Covenant on Civil and Political Rights (ICCPR)[58] guarantees that "No one shall be subjected to arbitrary or unlawful interference with his privacy…" This covers privacy in a broader sense as a right. However, the doubt still remains whether the criminal liability of privacy invasions in communication could be penalized. The European Convention on

[57] Mark E. Ells: 'A Brief Overview of Call Recording in California' <http://www.ellislawgrp.com/article13callrecordings.html> accessed 03 March 2020.
[58] Article 17 of the International Covenant on Civil and Political Rights of the United Nations of 1996.

Human Rights (ECHR)[59] guarantees that everyone has the right to respect for his private and family life, his home and his correspondence. It has been used to cover telephone tapping and use of bugging devices; it covers sexual life.[60]

Article 12 of the Universal Declaration of Human Rights (UDHR) enunciates that "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor attack upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks".

3.2. Literature Gap

The literature above discussed o far does not properly address the issue of telephone calls being recorded without consent or knowledge and used for a different purpose not intended by the parties. The voice or video communications/calls through mobile devices are not protected against using them for criminal activities by one of the parties to the conversation or a third party.

The legislations passed in the parliament does not protect or regulate information or communication through mobile devices which are currently in extensive use among the general public. Section 7 of the Computer Crimes Act No. 24 of 2007 makes it an offence and imposes punishment on any person who obtained information from a computer or a storage medium of a computer knowingly or having reason to believe that any other person has without lawful authority.

[59] Article 8 of ECHR.
[60] Perera K. S. "CCTV cameras: Is our privacy being encroached upon?" (2013) BALR Vol. XX p. 98

Sri Lanka Telecommunications Act No. 25 of 1991 provides for protection of data and regulates interception of telephone communications in sections 53 and 54 which is the only legislative enactment which provides some protection of data. However, the act is silent what action can be taken if and when any criminal invasion is done by the caller or receiver of such telephone communications.

Lack of a data protection authority or any form of governmental body to monitor and take actions in criminal invasions into data and privacy of communications causes great hardship in the country as the global development of technology enables anyone to invade into one's personal data in communications.

CHAPTER 4

DISCUSSION AND ANALYSIS

4.1. Introduction

The right to privacy in communication is an essential requirement in modern day technological development because it is easily susceptible to abuse by unknown people and hackers. It is high time that we amended existing laws or enacted new laws to protect individual privacy in exchange of data and conversation through mobile devices. When confidential telephone conversations are made public without the consent of the parties involved in the conversation, existing laws are inadequate to block, regulate and control such activities, so that introduction of new laws to protect privacy in communication through mobile devices is mandatory.

Recorded telephone calls could easily be made public by anyone through social media nowadays anonymously. If right to privacy in mobile communications is guaranteed as a fundamental right, everyone will be vigilant. Protecting of illegal and abusive phone calls and use of call recordings in committing offences or criminal activities should definitely be held criminally liable.

The recent alleged recordings and conversations included sensitive information which were made public affected society at large[61] and gave way to call to implement Right to Privacy Act in Sri Lanka.[62] As a result. Legal luminaries and activists have once again raised their concerns calling for a Right to Privacy Act in the country and the words of Weragoda were

[61] Hewajulige S, 'Ranjan's Audio Clips Rock Social Media' (2020) Daily Mirror <https://www.pressreader.com/sri-lanka/daily-mirror-sri-lanka/20200107/281500753181907> Accessed 12 June 2021; Voice clips include phone conversations with a lady judge, CID officers, politicians and various females Ranjan says used tactics to extract info, inspired by the movie Mafia.

[62] Anurangi Singh and Maneshka Borham, Sunday Observer [2020] <http://www.sundayobserver.lk/2020/01/12/alleged-recording-ranjan%E2%80%99s-conversations-call-implement-right-privacy-act> Accessed 12 June 2021.

that if you are having a conversation with me and if it is intended to be a conversation with me nobody else can be privy to that conversation. He urged the need for statutory law in voice recordings which is not provided for. Press Complaints Commission President Sukumar Rockwood states that to record someone without their consent is not professional.

4.2. Defining of Criminal Invasion of Privacy in Communication

Criminal invasion of privacy in communication is an unwelcome intrusion into another's domain without his or her knowledge and in this study, it is described and discussed relating to invasion of communication through mobile devices unlawfully. Once private and sensitive information is intercepted or recorded on a mobile device without the consent of the caller or receiver, it causes serious damage to the innocent party. When the information is made public without express consent or used to influence the caller for a wrongdoing with threat to make it public, it becomes criminal invasion.

California Penal Code makes it a crime for a person unlawfully to invade into someone else's privacy and the conviction carries a sentence of 6 months jail term and a fine up to $ 1000.00. Violations are categorized as by using a device to view someone inside a private room, by secretly photographing or recording a person's body under the clothing for sexual arousal, or by secretly recording or photographing someone in a private room to view that person's body.[63] The situation in California is supporting the study into criminal invasion of privacy in communication and the recording of telephone conversations without consent or knowledge and making it public.

[63] SCLG. 'Penal Code 647j PC – Criminal Invasion of Privacy in California' [2021] <https://www.shouselaw.com/ca/defense/penal-code/647j/> Accessed 22 June 2021.

4.3. Applicable Law in Privacy Protection in Sri Lanka

Invasion of privacy in communication commonly affects defaming character or good name of someone. Only applicable legal framework in Sri Lanka insists on the civil action to claim compensation. Long-dragged trials last for years to get relief for a victim in breach of privacy cases. Privacy rights are not considered as fundamental rights of citizen in terms of the Constitution, so that an aggrieved party cannot have expeditious relief for breach of fundamental rights and needs to resort to civil litigation. The defamation was criminal and actionable for a long time in the Penal Code, chapter XIX until it was repealed by the Penal Code (Amendment) Act No 12 of 2002.

4.4. Existing Law in Privacy Protection Sri Lanka

The common law in Sri Lanka does not recognize any right to the protection of personal information. It only permits peripheral protection or remedial action for invasion of privacy stemming from inappropriate use of personal data.[64]

Existing legal framework in regard to the privacy in communication and protection can be found in some of legislative enactments;

i. Constitution of Sri Lanka,
ii. Penal Code,
iii. Evidence (Special Provisions) Act No 14 of 1995,
iv. Electronic Transactions Act No 19 of 2006,
v. Telecommunications Act No 25 of 1991, and
vi. Computer Crimes Act No 24 of 2007.

[64] 'EPIC – Privacy and Human Rights Report' (2006) <http://www.worldlii.org/int/journals/EPICPrivHR/2006/PHR2006-Republic-28.html> Accessed 20 June 2021.

4.4.1. The Constitution of Democratic Socialist Republic of Sri Lanka 1978

Article 14 (1) (a) protects the freedom of speech and expression including publication as a fundamental right, subject to limitations in Article 15 (7) in the interests of national security, public order and the protection of public health or morality, or securing due recognition and respect for the rights and freedoms of others.

4.4.2. The Penal Code

Penal Code is the main legislative enactment of defining offences and punishments in Sri Lanka which was drafted more than 130 years ago in 1883. The laws should change as the needs of people and the society change over time while new offences are created. Amendments have not been brought into the code to protect privacy in communication through mobile devices. Mobile phones were invented around 1970s and Sri Lanka began cellular telephone services around 1989.

However, Section 22 of the Penal Code (Amendment) Act No 22 of 1995 restricts the printing and publication of any matter which may make known the identity, of any person against whom an offence under section 345, or 360A, or 360B, or 363, or 364A, or 365 or 365A, or 365B is alleged or found to have been committed (victim). All these are sexual offences so that privacy rights of individual are protected in such cases.

4.4.3. The Evidence (Special Provisions) Act No 14 of 1995

This gives legal protection for voice or video recordings, and telephone call recordings as well as any type of contemporaneous recordings in the electronic form.[65]

[65] Evidence (Special Provisions Act No 14 of 1995. s. 4 (1).

The Part II of the Act also protects computer evidence; any information contained in any statement produced by a computer[66]. A special procedure[67] is mentioned to produce such evidence in a court case where original has to be retained by the person who intends to produce it and to be proved. These legal provisions are still applicable although Electronic Transaction Act came into force in 2006.[68] The provisions of this Act can be applied to prove any communications through mobile phones if the original is retained in a form which can be accessed later and without editing or tampering.

4.4.4 The Electronic Transactions Act No 19 of 2006

This was enacted for securing data and communications in use of evidence and in court cases. This mainly focuses on the electronic evidence to facilitate domestic and international electronic commerce,[69] rather than protecting individual privacy in communication. However, data contained in emails, text messages, electronic recordings or other communication are given legal recognition in the act to prove civil or criminal cases. The interpretation of "communication" in the Act[70] is limited to any statement, declaration, demand, notice or request, including an offer in connection with an electronic transaction. However, "information" includes text, messages, data, voice, sound, database, video, signals, software, and computer programs. The term "electronic transaction" is not defined in the act although the word "electronic" is defined.

[66] Evidence (Special Provisions Act No 14 of 1995. s. 4 (1). s. 5 (1).
[67] ibid 66. s. 7 (1). The party proposing to tender such evidence shall, not later than forty-five days before the date fixed for inquiry or trial file, or cause to be filed, in court, after notice to the opposing party…
[68] Electronic Transactions Act No 19 of 2006. s. 22. Nothing contained in the Evidence (Special Provisions) Act No 14 of 1995 shall apply to and in relation to any data message, electronic document, electronic record or other document to which the provisions of this Act apply.
[69] Ibid 68 s. 2.
[70] Ibid 68. s. 26.

This Act is a development of the use of electronic evidence in courts and a fulfillment of a long-term requirement in the use of digital evidence and data. The possibility in protecting electronic evidence strengthens the protection of privacy rights as one can prove the original recordings in court when it is invaded by a third party violating the personal liberty of the citizen.

The Electronic Transactions Act will ensure greater legal certainty for e-Commerce and e-Business providers, and legal validity for other international legal instruments, and defines the time and place of dispatch and receipt of electronic communications between contracting parties, tailoring traditional contract rules to transform into the digital era[71]. Accordingly, the electronic evidence gained legality in court proceedings. This will facilitate in initiating legal action with the use of digital evidence, such as phone call recordings against violators.

4.4.5. Computer Crimes Act No 24 of 2007

This was enacted to protect data and information transferred through computers. It provides protection for the information of any person in making it a punishable offence to deal with information obtained from a computer[72]. The protection and coverage in the Act, if extended to the communication through mobile devices or tab phones, this can be utilized to protect the privacy of individuals.

Section 8 of the Computer Crimes Act provides protection of information, traffic data and any communication through computers and makes illegal use of them an offence. Although

[71] ICTA 'Enabling Digital Laws' <https://www.icta.lk/act/> Accessed 24 July 2021.

[72] Computer Crimes Act No 24 of 2007. s. 7. Any person who, knowingly or having reasons to believe that any other person has without lawful authority obtained information from a computer or a storage medium of a computer- (a) buys, receives, retains, sells, or in any manner deals with; or (b) offers to buy, or sell, or in any manner deals with; or (c) downloads, uploads, copies or acquires the substance or meaning of, any such information shall be guilty of an offence.

this protects computer communication, such as; zoom, skype and internet calls, this does not cover privacy rights in communication through mobile devices. Section 38 interprets that "information" includes data, text, images, sound, codes, computer programs, databases or microfilm. This definition is different from the interpretation given for information in the Electronic Transactions Act although similar legal aspects are visible in both enactments.

4.4.6. Sri Lanka Telecommunications Act No 25 of 1991

This was enacted to supplement protection for telecommunications in Sri Lanka which strengthens this study, although it does not protect privacy rights in mobile communication. The inclusion of provisions for protection of phone call in this digital era is a must. The Act was passed in Parliament in 1991 when there were very few mobile communications in Sri Lanka. This Act provides protection for interception of telecommunication transmission.[73] Section 54 of the Act makes it an offence for interception and disclosure of contents of messages by telecommunication officer. The protection of communication through mobile devices needs to be included in this enactment.

4.4.7. Draft Laws and Privacy

The Cyber Security Bill was drafted to protect vital information and essential services from cyber-attacks, and the Data Protection Bill aims to protect personal data and regulate its processing under overarching constitutional right to information and corresponding right to privacy.[74] It defines personal data, special categories of data, and processing and controlling of data. This is a timely need which did not become a reality yet. Laws are drafted and bills

[73] Telecommunications Act No. 25 of 1991. s. 53. Every person who willfully seeks to intercept and improperly acquaint himself with the contents of any telecommunication transmission not intended for general reception shall be guilty of an offence.

[74] Singh V. 'Sri Lanka: Introduction to Digital security Laws in Sri Lanka' (2020) <https://www.mondaq.com/security/879840/introduction-to-digital-security-laws-in-sri-lanka> Accessed 24 July 2021.

are prepared, but necessary approvals yet to be taken before they are being presented to the parliament. The writer raises a vital issue as to the security of information when South Asia becomes increasingly digitalized from freedom of speech and surveillance.

Senaratne N. said increased digitization of the economy in the use of smartphones is generating large amounts of data from the 6.2 million internet users in Sri Lanka, requiring laws to protect personal data.[75] The existing Electronic Transaction Act of 2006 and the Computer Crimes Act of 2007 facilitate e- commerce, but are not sufficient in privacy and data protection. This is acceptable on privacy protection in this digital era because there are no specific laws to protect individual privacy.

She suggests that use of Virtual Private Networks (VPN) is risky to privacy when the country is in states of emergency with bans on social media. The use of Virtual Private Networks (VPN) also brings in privacy concerns. In certain cases, applications providing this service for free, sell consumer internet activity data to advertisement targeting agencies. VPNs can capture all data that are being transmitted or received by a device, the information captured can be very detailed (unencrypted messaging services, location, contact information, app usage) and can easily be personally identifiable.[76] This directly affects privacy of individuals in protecting his/her personal communications which requires that the laws should be strict for the protection of personal data from unauthorized access by third parties.

[75] 'Sri Lanka's draft data protection and privacy laws should not hamper markets, innovation: IPs' (2019) economynext<https://economynext.com/sri-lankas-draft-data-protection-and-privacy-laws-should-not-hamper-markets-innovation-ips-30995/> Accessed 03 August 2021

[76] Nuwanthi Senaratne N, 'The Growing Need for Privacy and Data Protection in Sri Lanka' (2020) TALKING ECONOMICS. <https://www.ips.lk/talkingeconomics/2020/01/13/the-growing-need-for-privacy-and-data-protection-in-sri-lanka/> Accessed 24 July 2021.

It is interesting to note in this article the writer confirms that out of 107 countries 21% have no legislation around privacy and data protection, including Sri Lanka and although the existing Electronic Transaction Act and the Computer Crimes Act facilitate e-commerce, they do not provide for sufficient privacy and data protection.

4.5. Analysis of the Available Studies, Judgments and Articles

The available studies in this respect lacks protection of personal communications which take place on mobile devices. The concerns are directed for privacy in day-to-day communications of the citizen which can be intercepted by state organs or individuals or can be made use of criminal purposes in blackmailing and victimizing the innocent party. There is no legal study directly focused on this aspect although some concerns were made in certain legislative provisions as discussed above. There is no protection of privacy in personal communications through mobile devices which are being used widely in the country in business or private nature and recorded. The recording of phone calls and conversations is not illegal in Sri Lanka as there is no law to monitor or restrict the same.

The practice of making recorded calls public should be restricted by enacting necessary legislation because the innocent citizen will be in danger. The unnecessary frightening of the public with recording of personal telephone conversations was discussed in a recent news article[77]. ITS President Rajeev Mathew said that several print and electronic media were seen attempting to emphasize that recording phone conversations is illegal. *"We inform the public that it is impractical to ban the recording of personal telephone conversations and request all media institutions not to frighten the public unnecessarily.*"[78]

[77] Lahiru Fernando, 'Recording of phone conversations is not illegal under Lankan law' (23 January 2020) <https://www.dailynews.lk/2020/01/23/local/209188/%E2%80%98recording-phone-conversations-not-illegal-under-lankan-law%E2%80%99> Accessed 23 June 2021
[78] ibid 77

This article emphasizes the fact that recording of telephone conversations is not restricted or limited. The benefits gained by such call recordings are summarized as being helpful to net criminals. the reduction of crime rate, and a means to tackle with criminals. These advantages become disadvantages when someone gets use of it for criminal purposes.

Privacy was discussed in several authorities in the Supreme Court of Sri Lanka, however, there is yet no clear protection guaranteed to the citizen in his/her private communications over the phone. In the case of *Dr. Nalin de Silva v Ranil Wickramasinghe and Others,*[79] Article 14A of the Constitution was reproduced as was introduced by the Nineteenth Amendment to the Constitution declared that no restrictions shall be placed on the right of access to any information, other than such restrictions prescribed by law as are necessary in a democratic society. national security, public safety, prevention of crime, protection of health or morals and reputation or rights of others, privacy etc. However, the case was dismissed by holding that the petitioner had failed to satisfy the court any breach of his fundamental rights of the executive or administrative action. Here it is not considered what privacy of citizen is or how the privacy and freedom of expression are separated. Although Article 14A was enacted, it is still subject to restrictions in the Article 15 (7).

Almost everyone currently uses a mobile device to communicate with others. This development risks some individuals who use the mobile devices without basic knowledge of technology. Cloning attacks launched by criminals simply captured and reprogrammed secret user identifier into their own phones, which resulted in development of advanced security services for the second-generation mobile systems (GSM and IS-95) and third-generation systems.[80]

[79] S.C. FR Application No. 308/2015 decided on 02 February 2017.

[80] J Rodrigues, Kai Lin and Jaime Lioret, 'Mobile Networks and Cloud Convergence for Progressive Services and Applications' (2013) Ch. 4. International Science Reference

Network security is defined as the protection of networks and their services from unauthorized access, modification, destruction or disclosure by the authors of the same work. Once the network security is established, the communication may take place with respect to privacy of individuals. Network providers should be held responsible for not giving necessary protection in communications and allowing third parties to have access or interception.

4. 6. Production of Electronic Evidence in Courts and Privacy

Current legal framework for production of electronic based evidence in courts are based on two legislations, namely the Evidence (Special Provisions) Act No 14 of 1995 and the Electronic Transactions Act No 19 of 2006, both of which are complementary each other in nature. These legal enactments harmonizing with the Evidence Ordinance have to be used in proof of privacy violation trials on call recordings of private communications. In terms of Section 6 of the Evidence (Special Provisions) 14 of 1995, computer printouts could be produced, if they are accompanied by an affidavit of a person occupying a responsible position in relation to the operation of the relevant machine.[81] It was decided that photographs, and other forms of contemporaneous recordings, have been admissible in evidence in Sri Lanka despite the limitations of Section 3 of the Evidence Ordinance which confined its definition of "evidence" to oral and documentary evidence, and Section 165, which empowered court to order the production in court of anything, to admit in evidence, contemporaneous recordings of public speeches, telephone conversations preserved through wire or a tape recording, and photographs.[82] There still remains some difficulties in producing such electronic evidence in regard to the authenticity and genuineness. Section 4 (1) (a) to (d), of the Evidence (Special Provisions) 14 of 1995 have to be complied with.[83]

[81] Kiran Atapattu Vs Pan Asia Bank Limited (2000) 2 SLR 276
[82] Upali Dharmasiri Welaratne Vs. Wesley Jeyaraj Moses (S.C. Appeal No. 65/2003 decided on 27 May 2009)
[83] Abeygunawardane Vs. Samoon and Others (2007) 1 SLR 276

4.7. Lessons from Selected Jurisdictions

Selected jurisdictions in this study were India and the US where new lessons for digital privacy rights in communication could be elaborated. State of California introduced a sweeping law protecting digital privacy rights[84] in the Electronic Communications Privacy Act which bars any state law enforcement agency or other investigative entity from compelling a business to turn over digital communications without a warrant – including emails, texts, documents stored in the cloud and to track location of electronic devices like mobile phones. Restrictions should be imposed on the access to cloud storage in a mobile phone by the service provider or any government agency.

The evaluation of the two jurisdictions suggests that privacy protection is essential in digital world and it should be legally established through interpretation of the current provisions in the constitution to include it as a fundamental right. Judges should be careful in analyzing the law where their judgements finally remain authoritative over years and people suffer or benefit.

[84] Wired. 'California Now Has the Nation's Best Digital Privacy Law' [2015] <https://www.wired.com/2015/10/california-now-nations-best-digital-privacy-law/> Accessed 14th June 2021.

CHAPTER 5

FINDINGS AND RECOMMENDATIONS

5.1 Findings

The main impetus for this thesis was the non-availability of protection for communication through mobile devices which are in common use today. This thesis found that there was legislation providing protection of data and information stored in computers, and interception of calls, however, there was no guarantee of protection for personal and private phone calls which are recorded and made public without knowledge or consent of the caller or receiver as the case may be. The privacy of individuals in communication is not even a fundamental right in Sri Lanka, although restrictions are included on the freedom of expression.

This thesis identified the imposition of penal sanction for the offence of criminal invasion of privacy in communication would minimize crime rate by establishing the fear within the population to commit such invasion. Penal laws were identified as not covering to regulate and punish those who violate one's privacy in communication. The individual's right of privacy in communication should have been made a fundamental right in the Constitution of Sri Lanka.

This study was then directed to analyze the situation in India and the U.S. in order to find the relevant constitutional and legislative provisions with judgments in protecting the privacy in communication.

It was further found that there is no encryption of data in many social media chats and in communication which is converted into a code preventing unauthorized access by third

parties. End-to-end encryption is a method of secure communication that prevents third parties from accessing data while it is transferred from one end system or device to another where data is encrypted on the sender's system or device and only the intended recipient can decrypt it[85].

The right to privacy is generally accepted throughout the democratic world as a basic fundamental human right and privacy effectively is a limited, but a fundamental right, universally guaranteed[86]. The writer in this article expresses that it is essentially a privilege granted to individuals to protect their actions, choices and private opinions shared in the personal sphere from being exposed or scrutinized by the world at large. The article analyzes the legal background in two jurisdictions, namely; India and America. It is accepted in the world that the privacy should be a fundamental human right as a novel concept which should be included in the constitution and the Supreme Court should recommend this to be included in the constitution in their opinion.

5.2 Recommendations

There is no protection of individual privacy in communication through mobile devices and in effect, it is open for invasion by media personnel, politicians and third parties. Introduction of necessary amendments to the existing laws to punish for criminal invasion of privacy is mandatory in the Penal Code. Criminal sanction should be imposed in order to have a safer society with free communication and to reduce crime rate. When private and confidential communication or a recorded phone conversation is made public by caller, receiver, media or

[85] Ben Lutkevich and Madelyn Bacon, 'End-to-end encryption (E2EE)' SearchSecurity <https://searchsecurity.techtarget.com/definition/end-to-end-encryption-E2EE> Accessed 27 July 2021.
[86] Agnidipto Tarafder 'Surveillance, Privacy and Technology: A Comparative Critique of the Law of USA and India' (2015) Vol. 57. No. 4 Journal of the Indian Law Institute. <https://www.jstor.org/stable/44782800> Accessed 31 July 2021.

third party, he/she should be made criminally liable in order to curtail major social issues such as family break-ups, blackmails and suicides.

The privacy is a basic fundamental human right according to the international conventions and analytical studies, so that it shall be included in the Constitution of Sri Lanka under the fundamental rights chapter without any limitation because the technology development allows criminals to intrude into the personal domain of others.

The end-to-end encryption of data in communication is recommended in social media platforms, so that privacy of individual communications is digitally protected from invasion by third parties. This could be done by the service providers; however, it is not yet seen any established end-to-end encryption in phone calls through mobile devices.

An Independent Data Protection Authority needs to be implemented in the country which can take immediate actions in violation and criminal invasion of personal data in the use of social media as well as in communications. Sri Lanka Computer Readiness Team (SLCERT) refers the complaints of individuals to Criminal Investigations Department or informs the victim to refer the action to the nearest police station after they first entertain such complaints. A Data Protection Authority can be monitor SLCERT in initiating criminal prosecutions in the relevant court without delay. The Data Protection Authority should be entrusted with necessary powers to summon any person and inquire into any type of data and privacy violations in communications among other ancillary activities.

CHAPTER 6

CONCLUSION

6.1 Executive Summary

The background of the research starts with the history of mobile phone communication and networks with the emerging the social issues when privacy of individual is invaded by a third party. Selected jurisdictions for compassion were India and United States of America in which both countries practice common law principles similar to Sri Lanka.

It is necessary to protect privacy rights of the citizen by the government as the smooth running of the society needs protection of individual rights of privacy without intervention by government or third parties. Data protection legislation being passed in the parliament would facilitate in overcoming this issue while resolving challenges as mentioned by De Soyza[87] such as, balancing of the freedom of expression and the right to privacy. This issue must be addressed when data protection is legalized in order to harmonize with the freedom of expression which is a fundamental right in the Constitution of Sri Lanka. The restrictions on the right of expression are already imposed in the interests of national security, public order, and the protection of public health or morality, or for the purpose of securing the recognition and respect for the rights and freedoms of others under Article 15 (7) of the Constitution.

When States ratify treaties or declarations, such as the ones mentioned above, they obligate themselves to respect, protect and fulfil the rights enshrined within those instruments.[88] De Soyza further comments on the United Nations General Assembly resolution on the Right to Privacy in the Digital Age that governments, companies and individuals can have

[87] Samantha de Soyza, 'The right to privacy and data protection act: Need of the hour' [2017] <https://www.ft.lk/article/606874/The-right-to-privacy-and-a-data-protection-act:-Need-of-the-hour> Accessed 20 June 2021.
[88] ibid 87.

surveillance, interception, and data collection violating human rights, in particular the right to privacy. Quotation of *"the rights held by people offline must also be protected online"* is of much importance. When information held by an individual is conveyed via telephone, or other means, it goes with the risk of publication or unprotected from the time it is being communicated and it should be protected by law.

Inadequacy of necessary protection for privacy is visible in the legal framework in Sri Lanka and the need for protection has arisen in the recent past with the development and extreme use of mobile devices. The criminal invasion of privacy is discussed in detail to include it as a punishable offence in the penal laws of Sri Lanka.

The need of legislation protecting privacy rights is discussed at length throughout the research and it was recently addressed in United Nations General Assembly. Human Rights Council on 18 May 2021 Forty-seventh Session.[89] The International Conventions and Treaties require the protection of individual privacy and Sri Lanka also has ratified to many such treaties. These ratifications should be legalized in Sri Lanka with necessary legislation passed in the parliament. Digital development in communication has to be legalized to control crimes and serious problems in a peaceful society by the state. When it comes to legalize and protect privacy of individual, any state faces concerns over the balance between national security and privacy as well as between freedom of expression and protection of privacy rights.

[89] UN General Assembly. Human Rights Council 'The Right to Privacy in the Digital Age' [2021] Human Rights Council requested UN High Commissioner to prepare a hematic report on how artificial intelligence, including profiling, automated decision making, and machine-learning technologies may, without proper safeguards, after the enjoyment of the right to privacy, and to submit it to the Council at its forty-fifth session.

Legality of call recordings depends on the applicable laws in the relevant jurisdictions. In India, there are no clear legislative provisions regulating telephone calls and whether only one-party or two-party consent is needed in recording such calls.[90] In the United States. call recording is generally legal at federal level on a single consent basis, but there are differences between individual states.[91] In California in the US, all-party consent is generally needed for recording of phone calls, however section 632.7 of the Penal Code states that recording conversations where either party is on a cell phone or cordless phone without a warning is illegal.[92]

In Sri Lanka, there is no law regulating phone call recordings even with one-part or all-party consent. The issue arises when it is recorded and used later to gain illegal benefit. Fabricated call recordings may also be used to commit crimes, and force or influence innocent people to commit crimes if the call recording is not regulated by the government authorities and made illegal acts prosecuted. In a press release,[93] it was stated that even though the authenticity and source of these recordings remain uncorroborated, a number of these recordings are being circulated through social media platforms like wildfire without being subjected to any form of control whatsoever. This is in line with fundamental rights of citizen under the Constitution of Sri Lanka, however, the right to privacy is not included with express provisions.

[90] Maria Sundstrom 'Is It Legal to Record Calls? A Global Guide for Sales Leaders' [2021] <https://www.salestrail.io/blog/is-call-recording-legal-a-complete-guide-for-sales> Accessed 25 June 2021.
[91] ibid 90.
[92] Angela Goldman, 'California Recording Laws: Can I Legally Record Sales Calls?' (2018) Execvision <https://www.execvision.io/blog/california-compliant-call-recording/> Accessed 25 June 2021.
[93] Sumudu Chamara, 'Do We Have the Right to Privacy?' (2017) CeylonToday <https://archive.ceylontoday.lk/print-more/50553> Accessed 25 June 2021.

The literature above discussed relating to the privacy mainly focuses on the communication through computer and data, although it takes place in mobile devices through voice calls with the use of data or GSM networks. Communications through computers are found in skype calls, emails, google meetings, zoom meetings and various applications. These calls and communications can also be recorded by either party while emails are stored in the email folders in the system itself. The legal protection is amply provided for computer-based data protection currently in various legislations. When the technology develops, the law should be amended or new laws should be introduced to protect the privacy and balance the freedom of speech and expression. These two situations are complementary where the state should balance the privacy with the right to expression. National security is one of the main factors most governments take use of, in order to invade one's privacy in communications. This was commented by the Supreme Court of Sri Lanka in *Leader Publications (Pvt) Limited v. Ariya Rupasinghe*[94] as Article 19 of the UDHR, binding on all States proclaims the right to freedom of expression and Article 19 of the ICCPR.

International conventions and treaties are also valuable in this regard when Sri Lanka has ratified to them, however, being a dualist country ratification would not be sufficient. Necessary legislation needs to be drafted and passed in parliament in order to include in the laws of the country and to have practical effect.

[94] S.C (F/R) No. 362/2000. Written Comments Submitted by Article 19 Global Campaign for Free Expression. June 2000. These brief reviews national security and public order restrictions on freedom of expression and how such restrictions have been dealt with under both international and comparative law.

Relevant judgements in the field of privacy rights are of great importance as they become laws once decided by the Supreme Court of Sri Lanka in analysing legal and Constitutional provisions.

Subscribers have direct access to wireless cellular networks increasing threats and the security of cellular networks still remain highly outdated and insecure.[95] This author publishes a collection of articles in which the cellular networks and security are described at length; however, the privacy concerns are not addressed to a considerable extent in the book. It is the privacy which can have a latter effect on the subscriber in interception losing the privacy.[96] When there is no proper security in cellular networks, the subscribers are being victimized in acts of privacy violations if preventive measures are not taken in any legal regime.

Finally, it is interesting to note what *"privacy self-management"* is. The data protection legal framework is there to provide individuals against privacy infringements, but individuals themselves also have a responsibility (and capabilities) in protecting their privacy.[97] This approach is appreciated as the responsibility of each and every individual for privacy self-management should be promoted in reducing the impact on its violations.

[95] Peng Liu, Thomas F La Porta and Kameswari Kotapati, "Cellular Networks Security" in Vacca J R, *Networks and System Security* (Elsevier Inc 2009)
[96] ibid 95
[97] Serge Gutwirth, Ronald Leenes and Paul De Hert, *Data Protection on the Move* Vol. 24 (Springer Dordrecht Heidelberg 2016

6.2 Further research

Further research on digitalization of communications in Sri Lanka and safeguard for privacy should be carried out as the current Constitutional provisions do not guarantee it as a fundamental right and citizens have lost the confidence in communication through any media. Constitutional framework should be reviewed in order to include privacy as a basic human right in the fundamental rights chapter without any limitation clauses.

It would be beneficial to research further how the electronic evidence could be applicable in legal suits to prove the invasion of privacy by production of call recordings where genuineness of them would be at issue, and how to bring forward legislations in Parliament of Sri Lanka to protect individual privacy and penalize for the offences in violating privacy whether it would be an amendment to the Penal Code or new piece of legislation.

BIBLIOGRAPHY

LEGISLATION / STATUTES

Computer Crimes Act No 24 of 2007.

Electronic Transactions Act No 19 of 2006.

Evidence (Special Provisions Act No 14 of 1995.

Information Technology Act (India)

Penal Code (Amendment) Act No 22 of 1995

Privacy Act in the USA

Sri Lanka Telecommunications Act No. 25 of 1991

The Constitution of the Democratic Socialist Republic of Sri Lanka.

INTERNATIONAL CONVENTIONS

American Convention on Human Rights.

Budapest Cyber-Crime Convention.

European Convention of Human Rights.

European Convention for the Protection of Human Rights and Fundamental Freedom.

International Covenant on Civil and Political Rights of the United Nations of 1996.

Universal Declaration of Human Rights.

DECIDED CASES

Devinda Abeynayake (BALR (2011) Vol XVII p 138)

Dr. Nalin de Silva v Ranil Wickramasinghe and Others (S.C. FR Application No. 308/2015)

Hewamanna v Attorney General (1999) 'EPIC – Privacy and Human Rights Report' (2006) <http://www.worldlii.org/int/journals/EPICPrivHR/2006/PHR2006-Republic-28.html> Accessed 20 June 2021.

Hewamanne v. De Silva and another (1983 (1) SLR 1)

Justice K. S. Puttaswamy (Retd) vs Union of India (Writ Petition (Civil) No. 494 of 2012 decided on 24 August 2017)

Leader Publications (Pvt) Limited v. Ariya Rupasinghe (S.C (F/R) No. 362/2000)

Nadarajah v Obeysekera [52NLR76] (1971)

People's Union of Civil Liberties v Union of India (AIR 1997 (SC) 568)

Rayala M. Bhuvaneswari vs. Nagaphanender Rayala (AIR 2008 AP 98)

Sinha Ranatunga v. State (2000 (2) SLR 172)

BOOKS

Bnskill J and McKie D, *Your Right to Privacy* (International Self-Counsel Press Ltd 2016)

Gutwirth S, Leenes R and De Hert P, *Data Protection on the Move* Vol. 24 (Springer Dordrecht Heidelberg 2016)

Liu P, Thomas F, La Porta, "Cellular Networks Security" in Vacca J R, *Networks and System Security* (Elsevier Inc 2009)

Nagpal R. *Data Privacy Law (India)* (Asian School of Cyber Laws 2012)

Theresa M. Payton, and Theodore Claypoole, *Privacy in the Age of Big Data* (Rowman & Littlefield 2014)

Warren S D & Brandeis L D, *The Right to Privacy* Vol. IV (Harvard Law Review Association 1890)

RESEARCH JOURNAL ARTICLES AND REPORTS

Dalmia V P, 'Phone Tapping and Recording of Telephonic Conversation- Right to Privacy and Indian Law' [2018] <https://www.mondaq.com/india/Privacy/707096/Phone-Tapping-And-Recording-Of-Telephonic-Conversations-Right-To-Privacy-And-Indian-Law> Accessed 03 March 2021.

Santosh D, *'Mobile Phone Communication Technology'* [2009] <http://www.mobilecellphonerepairing.com/mobile-phone-communication-technology.html> Accessed 28 May 2021.

Fernando L, 'Recording of phone conversations is not illegal under Lankan law' [2020] <https://www.dailynews.lk/2020/01/23/local/209188/%E2%80%98recording-phone-conversations-not-illegal-under-lankan-law%E2%80%99> Accessed 23 May 2021.

Goldman A, 'California Recoding Laws: Can I Legally Record Sales Calls?' (2018) Execvision <https://www.execvision.io/blog/california-compliant-call-recording/> Accessed 25 June 2021.

Perera K. S. ‘CCTV cameras: Is our privacy being encroached upon?’ (2013) BALR Vol. XX p. 98

Rishabh Arora, ‘A Critical Analysis on Data Protection and Privacy Issues in India’ Legal Service India E Journal. <https://www.legalserviceindia.com/legal/article-2705-a-critical-analysis-on-data-protection-and-privacy-issues-in-india.html> Accessed 3 March 2021.

Rodrigues J J P, Lin K and Lioret J, ‘Mobile Networks and Cloud Convergence for Progressive Services and Applications’ (2013) Ch. 4. International Science Reference

Senaratne N. ‘The Growing Need for Privacy and Data Protection in Sri Lanka’ (2020) TALKING ECONOMICS. <https://www.ips.lk/talkingeconomics/2020/01/13/the-growing-need-for-privacy-and-data-protection-in-sri-lanka/> Accessed 24 July 2021.

Singh S S, ‘Privacy and Data Protection in India: A Critical Assessment’ (2011) Vol. 53. Indian Law Institute <https://www.jstor.org/stable/45148583> Accessed 3 August 2021.

Singh V. ‘Sri Lanka: Introduction to Digital security Laws in Sri Lanka’ [2020] <https://www.mondaq.com/security/879840/introduction-to-digital-security-laws-in-sri-lanka> Accessed 24 July 2021.

Sooriyabandara V. ‘Balancing the Conflict between Right to Information and Right to Privacy under Sri Lankan Fundamental Rights Perspective’ (2016) Sabaragauwa University Journal.

Soyza S. D. ‘The right to privacy and data protection act: Need of the hour’ (2017) <https://www.ft.lk/article/606874/The-right-to-privacy-and-a-data-protection-act:-Need-of-the-hour> Accessed 20 June 2021.

Tajdar Jawaid, ‘Privacy Vs. National Security’ (July 2020) <https://arxiv.org/ftp/arxiv/papers/2007/2007.12633.pdf> Accessed 03 August 2021.

Tarafder A. ‘Surveillance, Privacy and Technology: A Comparative Critique of the Law of USA and India’ (2015) Vol. 57. No. 4 Journal of the Indian Law Institute. <https://www.jstor.org/stable/44782800> Accessed 31 July 2021.

Thomas Glaessner, Tom Kellermann and Valerie McNevin ‘Electronic Security: Risk Mitigation In Financial Transactions Public Policy Issues’ (2002) The World Bank <https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.119.8602&rep=rep1&type=pdf> Accessed 23 July 2021.

Wijekoon J. ‘Feature Story 2: Recent Developments in Data Protection Laws in the World and Personal Data Protection Law in Sri Lanka’

<https://www.juniorbarbasl.lk/assets/files/Feature%20Article%202.pdf> Accessed 3 August 2021.

WEB RESOURCES

Cambridge Dictionary. <https://dictionary.cambridge.org/> Accessed 1 July 2021.

Cataldo J. Quotetab. <https://www.quotetab.com/quotes/by-joseph-cataldo> Accessed 3 March 2021.

Chamara S. CeylonToday. 'Do We Have the Right to Privacy?' [2017] <https://archive.ceylontoday.lk/print-more/50553> Accessed 25 June 2021.

Definitions. <https://www.definitions.net/definition/intercept> Accessed 1 July 2021.

Global ICT Policies And Strategies And Indian Perspective by Global ICT Policy Formulation, Implementation and Its Performance Analysis <http://ptlb.in/iips/?p=405> Accessed 03 March.2020.

Heins M. 'The Right to be Let Alone: Privacy and Anonymity at the U.S. Supreme Court' (2010) <https://www.cairn.info/revue-francaise-d-etudes-americaines-2010-1-page-54.htm> Accessed 3 March 2021.

Hewajulige S, ‘Ranjan’s Audio Clips Rock Social Media’ (2020) Daily Mirror <https://www.pressreader.com/sri-lanka/daily-mirror-sri-lanka/20200107/281500753181907> Accessed 12 June 2021.

ICTA ‘Enabling Digital Laws’ <https://www.icta.lk/act/> Accessed 24 July 2021.

IEEE, ‘The Importance of Protecting the Privacy and Integrity of Data and Communication’ [2018] <https://www.prnewswire.com/news-releases/the-importance-of-protecting-the-privacy-and-integrity-of-data-and-communications-300671266.html> Accessed 28 may 2021.

Kaspersky Team, ‘What end-to-end encryption is, and why you need it’ (2020) <https://usa.kaspersky.com/blog/what-is-end-to-end-encryption/23288/> Accessed 26 June 2021.

Legal Information Institute ‘Invasion of Privacy’ <https://www.law.cornell.edu/constitution-conan/amendment-1/invasion-of-privacy> Accessed 03 August 2021.

Loshin P, ‘encrption’ <https://searchsecurity.techtarget.com/definition/encryption> Accessed 26 June 2021.

Lutkevich B and Bacon B, ‘End-to-end encryption (E2EE)’ SearchSecurity <https://searchsecurity.techtarget.com/definition/end-to-end-encryption-E2EE> Accessed 27 July 2021.

One Trust Data Guidance, ‘Sri Lanka – Data Protection Overview’ (March 2021) <https://www.dataguidance.com/notes/sri-lanka-data-protection-overview> Accessed 28 May 2021.

Pew Research Center ‘The State of Privacy in Snowden America’ [2018] <https://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/>

Maria Sundsrom ‘Is It Legal to Record Calls? A Global Guide for Sales Leaders’ [2021] <https://www.salestrail.io/blog/is-call-recording-legal-a-complete-guide-for-sales> Accessed 25 June 2021.

SCLG. ‘Penal Code 647j PC – Criminal Invasion of Privacy in California’ [2021] <https://www.shouselaw.com/ca/defense/penal-code/647j/> Accessed 22 June 2021.

‘Sri Lanka’s draft data protection and privacy laws should not hamper markets, innovation: IPs’ (2019) economynext<https://economynext.com/sri-lankas-draft-data-protection-and-privacy-laws-should-not-hamper-markets-innovation-ips-30995/> Accessed 3 August 2021.

Singh A. and Borham M. Sunday Observer. [2020] <http://www.sundayobserver.lk/2020/01/12/alleged-recording-ranjan%E2%80%99s-conversations-call-implement-right-privacy-act> Accessed 12 June 2021.

'EPIC – Privacy and Human Rights Report' (2006) <http://www.worldlii.org/int/journals/EPICPrivHR/2006/PHR2006-Republic-28.html> Accessed 20 June 2021.

Wired 'California Now Has the Nation's Best Digital Privacy Law' [2015] <https://www.wired.com/2015/10/california-now-nations-best-digital-privacy-law/> Accessed 14 June 2021.

UN General Assembly. Human Rights Council 'The Right to Privacy in the Digital Age' [2021].