September 2020

Right to Privacy in Sri Lanka

DISCUSSION PAPER
CENTRE FOR POLICY ALTERNATIVES

CENTRE FOR POLICY ALTERNATIVES
විකල්ප ප්‍රතිපත්ති මධ්‍යස්ථානය
மாற்றுக் கொள்கைகளுக்கான நிலையம்

The Centre for Policy Alternatives (CPA) is an independent, non-partisan organisation that focuses primarily on issues of governance and conflict resolution. Formed in 1996 in the firm belief that the vital contribution of civil society to the public policy debate is in need of strengthening, CPA is committed to programmes of research and advocacy through which public policy is critiqued, alternatives identified and disseminated.

No. 6/5, Layards Road, Colombo 5, Sri Lanka
Tel: +9411 2081384, +94112081385, +94112081386
Fax: +9411 2081388 Email: info@cpalanka.org
Web: www.cpalanka.org
Email: info@cpalanka.org
Facebook: www.facebook.com/cpasl
Twitter: @cpasl

ACKNOWLEDGEMENTS

This report was researched and written by Charya Samarakoon and Bhavani Fonseka. Comments on earlier drafts were provided by Dr Paikiasothy Saravanamuttu, Dr Asanga Welikala, Luwie Ganeshathasan, Khyati Wikramanayake, Nivedha Jeyaseelan and Kushmila Ranasinghe. The report was formatted by Ayudhya Gajanayake. CPA is grateful to all the individuals who supported the research by sharing information and insights.

Contents

I. Introduction

The right to privacy includes the right of individuals to lead their lives in a manner that is reasonably secluded from public scrutiny, and the right to make personal decisions regarding their lives. The importance of privacy and the multitude of practises through which privacy is breached are not fully appreciated by policymakers, businesses as well as the general public in Sri Lanka.

Proposed reform such as the revival of the National Register of Persons[1], recommendations for invasive surveillance methods[2] as well as violations of privacy in the wake of the COVID-19 pandemic[3] raises grave concerns, especially in the absence of legislative protection of the right to privacy in Sri Lanka. These developments, among others, need to be closely monitored, and wide debate and awareness generated on their potential implications and risks.

This paper discusses the importance of the right to privacy and seeks to critically respond to the above developments. It suggests that in order to effectively protect the right to privacy, it is essential to incorporate a justiciable right to privacy within the chapter of the Constitution on Fundamental Rights. However, this alone would not be sufficient as the meaningful enjoyment of a constitutional right to privacy would depend on access to legal remedies, an effective institutional framework as well as societal acceptance of the value of privacy.

The first section of the paper emphasizes the need for the right to privacy in a liberal constitutional democracy, identifying the effects of loss of privacy on individuals and society as well as arguments put forth for the protection of privacy by courts in local, comparative and international jurisdictions. The next section attempts to

[1] Economy Next, 'Sri Lanka President instructs to start work on digital database of citizens' *Economy Next* (Colombo) 13 May 2020 <https://economynext.com/sri-lanka-president-instructs-to-start-work-on-digital-database-of-citizens-69903/> accessed 22 June 2020.
[2] The Parliament of Sri Lanka, 'Report of the Sectoral Oversight Committee on National Security', 19 February 2020. <https://www.parliament.lk/uploads/comreports/1582610584075624.pdf#page=1> ;
[3] The violations of privacy in relation to the COVID-19 pandemic will be discussed in detail later in the report.

define the scope of the right to privacy, and suggest a framework for privacy protection with reference to comparative experience, international standards and best practices. The final section discusses the right to privacy in Sri Lanka, proposed and current legal frameworks affecting the right to privacy and potential threats to the right to privacy from administrative and policy reforms.

II. The Need for the Right to Privacy

The Public Value of the Right to Privacy

The debate on the constitutional protection of the right to privacy, the scope and extent of the right to privacy and how it should be balanced with other considerations such as the right to information, freedom of speech and expression, national security and public health is partly a debate on legal philosophy and partly a debate surrounding the utility and risks of recent technological innovations.[4]

However, privacy is not just a legal or technological issue but a complex social problem with many aspects. It follows then that there is no one definite legal or technological solution to address privacy violations. The effective protection of the right to privacy requires the involvement and contribution of a variety of groups and actors.

The concept of privacy as a legally protected right gained importance along with technological innovations which made the collection and storage of personal data easier and faster. With inventions such as Hollerith's punched card tabulating machine and telegraphy in the 19th century, concern about the interception of personal data and private communications increased.[5] Since then, legal innovations to protect privacy have been hard pressed to keep in step with the rapid technological advances in the field of data collection and processing.

It is often claimed that privacy is an individual concern that must be balanced against the common good.[6] Politicians and members of the intelligence community emphasize that especially when it comes to concerns of national security, 'there is a

[4] J. Rubenfeld, 'The Right of Privacy' [1989] 102(4) Harvard Law Review 737-807 ; R Shank, 'Privacy: History, Legal, Social, and Ethical Aspects ' [1986] 35(1) Library Trends <https://www.ideals.illinois.edu/handle/2142/7457> accessed 22 June 2020.

[5] R Shank, 'Privacy: History, Legal, Social, and Ethical Aspects ' [1986] 35(1) Library Trends <https://www.ideals.illinois.edu/handle/2142/7457> accessed 22 June 2020.

[6] D. E. Bambauer, 'Privacy versus Security' [2013] 103(3) Journal of Criminal Law and Criminology <https://scholarlycommons.law.northwestern.edu/jclc/vol103/iss3/2> accessed 23 June 2020. See also, A. Etzioni, The Limits of Privacy (1 edn, Basic Books 1999).

balance to be found between the individual right to privacy and the collective right to security.[7]'

However, this argument fails to take into consideration the diverse aspects of privacy and the social interests protected by the protection of individual privacy. Thus, it is argued that framing the debate in terms of individual versus collective rights is simplistic as well as misleading.[8]

The protection of individual privacy could directly improve the likelihood that public interests would be protected. For example, the privacy of individual medical records would make it more likely that individuals with diseases would seek help earlier, reducing the risk of infecting others and possibly preventing a strain on the health system.

It has been stated that the public value of privacy derives from the fact that it is a restraint on the arbitrary use of State power.[9] The right to privacy is essential for the meaningful fulfilment of a number of important civil and political rights, such as the freedom of expression, freedom of thought and belief, freedom of movement and association, right to a fair trial and due process protections, the right to be treated equally without discrimination and free and fair elections.

In a well-functioning democracy, those in power should be open and transparent about how their power is exercised. However, a similar degree of transparency must not be expected from individuals as the more transparent they are, the more vulnerable they may become to unjust treatment, discrimination and unequal

[7] Sir Malcolm Rifkind, Chair of the Intelligence and Security Committee (ISC) of the Parliament of the United Kingdom.

[8] TJ Maji, 'Fourteen Reasons Privacy Matters: A Multidisciplinary Review of Scholarly Literature' [2011] 81(2) The Library Quarterly <http://www.jstor.org/stable/10.1086/658870?origin=JSTOR-pdf> accessed 22 June 2020.

[9] A Marsoof, 'The Right to Privacy in the Information Era: A South Asian Perspective [2008] 5(3) SCRIPTed - A Journal of Law, Technology & Society <http://ssrn.com/abstract=1578222> accessed 22 June 2020. See also, DJ Solove and others, Information Privacy Law (Aspen Publishers 2006).

opportunities.[10] This is the balance between the right to information and the right to privacy which legislation on the right to information must seek to establish.[11]

The State often has great power over how personal data is collected and used and who has access to such data whereas individual citizens have no realistic power to make these decisions about their own personal data.[12] Due to this asymmetrical nature of surveillance, the mere existence of data gathering procedures by the State even in the absence of analysis or use of that data can be a violation of individuals' rights.[13]

An invisible prison

The 18th century utilitarian philosopher Jeremy Bentham proposed a design which he called the Panopticon for the construction of prisons. This structure was designed such that the inmates knew they were being watched but did not know whether they were being watched at a given time. Examining the effects of the Panopticon in his 1975 book 'Discipline and Punish: The Birth of the Prison', Michel Foucault states;

"The major effect of the Panopticon is to induce in the inmate a state of conscious and permanent visibility that assures the automatic functioning of power…by making the inmates the principle of [their] own subjection."

Thus, in the absence of a legally protected right to privacy, individuals live under the constant possibility of both overt and covert surveillance by a State which uses sophisticated technological innovations to gather, store and analyse personal data and even personal communications of its citizens. The citizens will, in effect, become the inmates of an invisible Panopticon where self-censorship and anticipatory conformity are adopted for survival.

[10] R Ratnasabapathy, 'Sri Lanka's plans to move to a digital ID promises benefits but carries grave risks' (*Echelon*, 3 October 2017) <https://www.echelon.lk/sri-lankas-plans-to-move-to-a-digital-id-promises-benefits-but-carries-grave-risks/> accessed 24 June 2020.

[11] In *Von Hannover v Germany*, the European Court of Human Rights acknowledged that "public figures must recognise that the special position they occupy in society – in many cases by choice – automatically entails increased pressure on their privacy."

[12] TJ Maji, 'Fourteen Reasons Privacy Matters: A Multidisciplinary Review of Scholarly Literature' [2011] 81(2) The Library Quarterly <http://www.jstor.org/stable/10.1086/658870?origin=JSTOR-pdf> accessed 22 June 2020. ; P Ewick and S Silbey, 'The Common Place of Law: Stories from Everyday Life' [1998] 28(6) Contemporary Sociology <DOI: 10.2307/2655592> accessed 26 June 2020.

[13] *S and Marper v United Kingdom* [2008] ECHR 1581.

The asymmetrical nature of state surveillance concentrates power within the bureaucracy, as it is virtually impossible for individuals to negotiate with the State on who has access to their personal information and how it will be used.[14] Thus it is submitted that the right to privacy must be legally protected and expecting government entities with considerably more bargaining power to self-regulate and use the data in their possession in good faith cannot work.[15]

[14] P Ewick and S Silbey, 'The Common Place of Law: Stories from Everyday Life' [1998] 28(6) Contemporary Sociology <DOI: 10.2307/2655592> accessed 26 June 2020.

[15] TJ Maji, 'Fourteen Reasons Privacy Matters: A Multidisciplinary Review of Scholarly Literature' [2011] 81(2) The Library Quarterly <http://www.jstor.org/stable/10.1086/658870?origin=JSTOR-pdf> accessed 22 June 2020.

What loss of privacy means for you: Debunking the 'if you have nothing to hide you have nothing to fear' myth

1. **Nuisance calls and harassment over the phone**

There are frequent reports of employees of various commercial establishments misusing their customers' mobile phone numbers to cause harassment. Strong privacy protections would compel businesses to ensure that their customers' contact details are handled securely.

2. **Details of family members**

Absence of privacy protections means that details of family members, including children, would be easily accessible to anyone. This would pose a greater risk once the proposed National Register of Persons with updated details of all family members is set up. This could also affect victims of domestic violence as individuals are required to update information such as change of address in the register as soon as there is any change of information.

3. **Health records**

Sri Lankan society attaches stigma to a variety of health conditions. At present, there are no laws protecting the privacy of health records which results in serious concerns on access to healthcare as well as discrimination of individuals based on health conditions or disability. This could also affect reproductive rights of individuals.[16]

4. **Employment, insurance, and financial services**

The absence of privacy allows large amounts of personal data to be collected and analysed using artificial intelligence systems to assess and categorize people, draw conclusions about their physical and mental characteristics, and predict their future medical conditions and their suitability for jobs. This can be used to assess their eligibility for employment, health care, insurance and financial services.

5. **Spam messages and emails**

Data is collected on a person's buying patterns using the system of customer loyalty cards. This data is used to direct spam messages and email for various products and services.

6. **Online financial fraud**

The absence of privacy protections means increased risk of identity theft, internet fraud and phishing.

7. **Cyber bullying**

There are frequent complaints of social media harassment, including misuse of personal photos and videos, use of fake accounts and social media accounts being hacked. Strong privacy protections would reduce the risk of cyber bullying.

8. **Extortion**

There is always the possibility of compromising personal communications or information being used for extortion. For instance, the absence of privacy protections preventing non-consensual recording of personal calls could result in this.

The loss of privacy affects all aspects of life of ordinary citizens. According to a study conducted by Sri Lanka CERT, over 33% of respondents reported receiving spam emails, while 25% reported social media and email accounts being hacked or someone creating a fake account under their name. Around 15% of respondents reported being victims of cyberbullying or their photos being used in an abusive way. **It has also been noted that women are disproportionately affected by loss of privacy.**

[16] The Centre for Policy Alternatives has previously highlighted this issue. See Centre for Policy Alternatives, 2007. *HIV / AIDS in Sri Lanka A Profile on Policy and Practice*. Centre for Policy Alternatives. Available at: <https://www.hivpolicy.org/Library/HPP001560.pdf>

Judicial Recognition of the Right to Privacy

The right to privacy is inextricably tied up with the integrity and dignity of the individual. Even before the right to privacy was enshrined in international human rights law documents, it was given judicial recognition as integral to the protection of an individual's autonomy and dignity. As *Entick v Carrington (1765)*[17] powerfully put it;

> "Ransacking a man's secret drawers and boxes to come at evidence against him, is like racking his body to come at his secret thoughts."

In common law legal systems, the right to privacy has been recognized as integral to the individual's dignity. In legal systems based on Roman Dutch Law too, the right to privacy has gained recognition as an independent personality right within the concept of *dignitas* and a breach of privacy would give rise to an action for injury under the *actio iniuriarum*.

Privacy has been emphasized as a means of protection from discrimination and persecution due to religious and political beliefs, health conditions, nationality and/or ethnicity, sexual orientation, as well as personal choices of an individual. This line of argument sees privacy as 'a tool to protect human dignity and esteem'.[18]

Judicial decisions in comparative jurisdictions have held that the right to privacy forms so fundamental a part in the dignity of the individual that it is inviolable unless the State can show by way of justification that some positive law has empowered or excused such violation.[19]

---

[17] *John Entick, (Clerk) v Nathan Carrington and Three Others*, [1765] EWHC KB J98, 95 ER 807.

[18] TJ Maji, 'Fourteen Reasons Privacy Matters: A Multidisciplinary Review of Scholarly Literature' [2011] 81(2) The Library Quarterly <http://www.jstor.org/stable/10.1086/658870?origin=JSTOR-pdf> accessed 22 June 2020. ; A Marsoof, 'The Right to Privacy in the Information Era: A South Asian Perspective [2008] 5(3) SCRIPTed - A Journal of Law, Technology & Society <http://ssrn.com/abstract=1578222> accessed 22 June 2020.

[19] *Entick v Carrington* [1765] EWHC KB J98, 95 ER 807 and *Griswold v Connecticut* 381 U.S. 479.

The counter-argument is that strong privacy protections, such as the constitutional protection of privacy as a fundamental right, could have an adverse effect on other rights such as the right to information and the freedom of expression as well as social interests such as national security and public health. In order to balance the protection of the right to privacy with such social interests, the State may invade upon an individual's privacy unless prohibited by some specific provision.[20]

The arguments put forth for the protection of privacy and the recognition of the value of privacy by courts in a few jurisdictions are discussed below.

Sri Lanka

The absence of the right to privacy in the fundamental rights chapter of the Constitution greatly undermines the protection of privacy in Sri Lanka. However, Sri Lankan courts have recognized the concept of privacy in limited circumstances. In *Chinnappa et al. v Kanakar et al*[21] the court recognised a right to household privacy in upholding a custom in the Jaffna peninsula, where adjoining landowners were permitted to enter the neighbour's land to protect his fence with the covering of *ola* leaves. In *Abraham v Hume*[22] it was recognized that the owner of an estate or a superintendent has no right to enter the labourer's lines and invade his privacy.

In *A.M.K Azeez v W.T Senevirathne (SI Police)*[23] the court convicted a husband and wife of insulting several police officers who had entered their house on suspicion that they were in possession of stolen goods. The Supreme Court in appeal reduced the sentence of the appellant having taken into consideration the circumstance in which the insulting comments were made (namely it being well after midnight and where the privacy and sleep of the accused appellant were disturbed).

The Supreme Court of Sri Lanka has further recognized that even in the absence of a constitutionally entrenched right to privacy, "*the importance which our Constitution*

[20] Black J's dissent in *Griswold v Connecticut* 381 U.S. 479.
[21] 13 NLR 157 at pages 158, 159 and 160.
[22] 52 NLR 449, at page 453.
[23] 69 NLR 209, at page 210.

attaches to the man's autonomous nature, through the guarantees of basic human rights (…) aimed at securing the integrity of the individual and his moral worth" would be violated by an invasion of the privacy of the individual, "*assail(ing) his integrity as a human being and thereby deny(ing) him his right to remain in society as a human being with human dignity.*"[24]

The approach of the Sri Lankan judiciary towards the subject of privacy shows that while the privacy of the home (spatial privacy) has been recognized in several instances, other aspects of privacy have received little to no consideration.

India

The constitution of India does not expressly protect the right to privacy and Indian courts have been reluctant to recognize an implied protection of the right to privacy. In *M P Sharma and Others v Satish Chandra, District Magistrate, Delhi and Others*,[25] the Supreme Court held that there is no justification to import the right to privacy "into a totally different fundamental right, by some process of strained construction."

However, subsequent decisions have taken a more liberal approach. In *Kharak Singh v The State of Uttar Pradesh and Others,*[26] Article 21 of the Constitution which ensures the protection of personal liberty was interpreted to include the 'right to be free from encroachments on his private life.' This position has been followed in *Rajagopal alias R.R. Gopal and another v State of T.N. and others.*[27]

These decisions paved the way for the 2017 judgment of the Supreme Court in *Justice K.S. Puttaswamy (Retd) vs Union of India*[28] which recognized the right to privacy as a fundamental right, mainly under Article 21 of the Constitution. This judgment was delivered in a challenge to the Indian biometric identity scheme Aadhaar. The decision in *Puttaswamy* paved the way for the decriminalization of homosexuality in India through the decision in *Navtej Singh Johar and others vs Union of India and*

[24] *Sinha Ratnatunge v State* [2001] 2 Sri L.R. 172.
[25] *M P Sharma and Others v Satish Chandra, District Magistrate, Delhi and Others*, AIR 1954 (SC) 300.
[26] *Kharak Singh v The State of Uttar Pradesh and Others*, AIR 1963 (SC) 1295
[27] *Rajagopal alias R.R. Gopal and another v State of T.N. and others*, AIR 1995 (SC) 264.
[28] Writ Petition (Civil) No 494 of 2012.

others,[29] demonstrating how the recognition of privacy as a fundamental right could have far reaching consequences in protecting both individual and social interests.

South Africa

The common law protection of the right to privacy stems from the Roman Dutch law *actio iniuriarum* in South Africa. In *O'Keeffe v Argus Printing and Publishing Company Ltd,* the Cape Supreme Court ruled that using a person's photograph for advertising purposes without consent constituted an aggression upon that person's *dignitas*.[30]

Following this case, the South African courts started to recognize the concept of privacy in a variety of circumstances including disclosure of a person's relationship with a celebrity[31], the publication of facts concerning the removal of children from the custody of their parents[32] and the disclosure by a doctor of the HIV-positive status of a patient.[33]

The courts have also recognised unreasonable intrusions into the private sphere as actionable. In *S v A*[34] and *Financial Mail Pty Ltd v Sage Holdings (Pty) Ltd*[35] it was recognized that recording personal conversations and listening to private telephone conversations was an invasion of privacy giving rise to a cause of action.

The 1996 Constitution of the Republic of South Africa protects privacy in Section 14, including the privacy of the person and home, possessions and communications. The Constitutional court in *Khumalo v Holomisa*[36], stated that 'no sharp lines' can be drawn between various facets of personality rights 'in giving effect to the value of human dignity in our Constitution', reiterating the essential role of privacy in maintaining human dignity.[37]

---

[29] Writ Petition (Criminal) No. 76 of 2016.
[30] *O'Keeffe v Argus Printing and Publishing Company Ltd* 1954 (3) SA 244 (C).
[31] *Mhlongo v Bailey* 1958 (1) SA 885 (E) and *National Media Ltd v Jooste* 1996 (3) SA 262 (A).
[32] *Rhodesian Printing and Publishing Co Ltd v Duggan* 1975 (1) SA 590 (R).
[33] *Jansen van Vuuren No v Kruger* 1993 (4) SA 842 (A).
[34] 1971 (2) SA 293 (T).
[35] 1993 (2) SA 451 (A).
[36] 2002 (5) SA 401 (CC) at para [27].
[37] J Burchell, 'The Legal Protection of Privacy in South Africa: A Transplantable Hybrid ' [2009] 13(1) Electronic Journal of Comparative Law.

The South African Supreme Court of Appeal has recently affirmed in *Grütter v Lombard*[38] the right to personal identity, including a person's likeness and name.

In *Mistry v Interim Medical and Dental Council of South Africa*[39] the Constitutional Court listed some general guidelines governing data protection, which have been followed in subsequent cases. The Protection of Personal Information Act (POPIA) was enacted in 2013 and came into effect from 1 July 2020. This Act codifies the current common law position in South Africa with regard to data protection. It acts as a detailed framework legislation supporting South Africa's constitutional right to privacy.[40]

The experience of South Africa is one of courts taking a progressive stance towards privacy which later translated into effective legislative reform, demonstrating the importance of an independent and progressive judiciary in the protection of privacy. The existing common law protections of privacy were applied in a variety of circumstances creating a robust body of jurisprudence on the right to privacy. The courts entrenched the right to privacy within the legal system as a fundamental right which was later incorporated into the Constitution in 1996. Similarly, even before data protection legislation was introduced, the courts recognized the value of personal data and gave expression to principles of data protection in their decisions. This was carried out in such a comprehensive manner that the eventual legislation on data protection is a codification of the common law position in South Africa with regard to data protection.

United Kingdom

In the United Kingdom, in *Douglas v Hello! Ltd*[41] privacy was recognised as a legal principle drawn from the fundamental value of personal autonomy. This position

[38] [2007] SCA 2 (RSA) at paras [8] to [13].
[39] 1998 (4) SA 1127 (CC).
[40] Hunton Andrews Kurth, 'South Africa's Protection of Personal Information Act, 2013, Goes into Effect July 1' (*The National Law Review*, 29 June 2020) <https://www.natlawreview.com/article/south-africa-s-protection-personal-information-act-2013-goes-effect-july-1> accessed 2 July 2020.
[41] [2005] EWCA Civ 595.

was followed in *Campbell v Mirror Group Newspapers Ltd*[42], holding that privacy lies at the heart of liberty in a modern state. "A proper degree of privacy is essential for the well-being and development of an individual."[43]

European Court of Human Rights

The European Court of Human Rights recognizes the importance of the right to privacy especially with reference to the collection of personal data by governments.

In *Klass v. Germany* (1978) it was ruled that:

"… in the mere existence of the legislation itself there is involved, for all those to whom the legislation could be applied, a menace of surveillance; this menace necessarily strikes at freedom of communication between users of the postal and telecommunication services and thereby constitutes an 'interference by a public authority' with the exercise of the applicants' right to respect for private and family life and for correspondence."[44]

In *S and Marper v. the United Kingdom* (2009) it was ruled that 'the mere retention and storing of personal data by public authorities, however obtained, are to be regarded as having a direct impact on the private-life interest of an individual concerned, irrespective of whether subsequent use is made of the data.'[45]

United States of America

In *Griswold v Connecticut* the Supreme Court of the United States found a right to privacy, derived from penumbras of other explicitly stated constitutional protections, mainly those granted by due process rights.[46] *Eisenstadt v Baird* (1971)[47] extended the right to privacy to be inherent in the individual, and not the marital couple as recognized in *Griswold,* making the right to privacy applicable in a wide variety of instances where individual choice was encroached upon by state action.

[42] [2004] UKHL 22.
[43] *Campbell v Mirror Group Newspapers Ltd* [2004] UKHL 22.
[44] *Klass and ors v Federal Republic of Germany* [1978] ECHR 4.
[45] *S and Marper v United Kingdom* [2008] ECHR 1581.
[46] *Griswold v Connecticut* 381 U.S. 479.
[47] 405 U.S. 438.

Roe v. Wade (1972)[48] and *Lawrence v. Texas* (2003)[49] used these rulings to uphold individual autonomy and restrict state intervention in personal decision making.

[48] 410 U.S. 113.

[49] 539 U.S. 558.

III. The Right to Privacy as a Fundamental Right

Scope of Privacy

Many jurisdictions including India and the United States have recognized privacy as an extension of other fundamental rights and protections such as the right to personal liberty and due process protections. This has served to protect privacy in the absence of a constitutionally entrenched right to privacy. However, this puts the right to privacy in a tenuous position where the protections offered could be reversed by a different judicial interpretation.

Additionally, the large variety of technological innovations which pose a threat to privacy may reduce the effectiveness of using already existing constitutional protections to protect the right to privacy. Extensions from the right to personal liberty and due process may fail to cover some instances where there is a clear violation of privacy.

It has also been argued that privacy is a moral right with a moral basis or justification rather than a legal or constitutional right derived from other rights.[50] Privacy is what links rational agency and moral autonomy. It is the link between making personal choices and acting upon those choices without the interference or influence of others. To break this link is to interfere with a person's capacity for self-government and self-determination.

The protection of the right to privacy is further complicated by the difficulties in specifying the scope of privacy. Privacy is a concept which lacks a single essence, and attempts to reduce it to a specific definition results in vagueness. It has been argued that privacy is best understood as 'a family resemblance concept in which various kinds of privacy disruptions are different from one another yet share important similarities.' The various aspects of privacy may seem different but are related to one another through a network of overlapping and criss-crossing

[50] M Alfino and G Mayes, 'Reconstructing the Right to Privacy' [2003] 29(1) Social Theory and Practice <https://www.jstor.org/stable/23559211> accessed 8 July 2020.

similarities, and thus, privacy may be used as an umbrella term for a related web of issues.[51]

Several authors who have dealt with privacy issues have distinguished between three spheres of privacy: informational privacy; physical, local or spatial privacy; and decisional privacy.[52] The regulation of the collection, storage and sharing of data concerns informational privacy. Spatial privacy is violated by practices such as live streaming, CCTV surveillance and the use of unmanned aerial vehicles (drones), which are not regulated by law in Sri Lanka. Decisional privacy is affected by the lack of all other forms of privacy and directly threatens the self-determination of individuals.[53]

Privacy is not an absolute right and may be restricted in the interests of other considerations. Under Article 4 of the International Covenant on Civil and Political Rights (ICCPR), States Parties to the Covenant may derogate from their obligations under the Covenant to the extent strictly required by the exigencies of the situation, provided that such measures are not inconsistent with their other obligations under international law and do not involve discrimination solely on the ground of race, colour, sex, language, religion or social origin.[54] The Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights states that restrictions on human rights under the ICCPR must meet the standards of legality, evidence-based necessity, proportionality, and

---

[51] TJ Maji, 'Fourteen Reasons Privacy Matters: A Multidisciplinary Review of Scholarly Literature' [2011] 81(2) The Library Quarterly <http://www.jstor.org/stable/10.1086/658870?origin=JSTOR-pdf> accessed 22 June 2020.

[52] DH Flaherty and G Mayes, 'On the Utility of Constitutional Rights to Privacy and Data Protection' [1991] 41(3) Case Western Reserve Law Review <https://scholarlycommons.law.case.edu/caselrev/vol41/iss3/14> accessed 8 July 2020. ; J DeCew, Judith. "Privacy." In *Stanford Encyclopedia of Philosophy*. Stanford, CA: Meta-physics Research Lab, Center for the Study of Language and Information, StanfordUniversity, 2006. <http://plato.stanford.edu/entries/privacy/>.

[53] 'Hypernudging' in self-tracking technologies is an example of the dependence of decisional privacy on informational privacy. For example, Uber 's (offline) collection of real-time data in order to predict your next ride and tailor on-the-go recommendations based on one's location and past choices. Similarly, individuals' decisional privacy on reproductive rights may be affected by the absence of physical privacy (*Roe v Wade* 410 U.S. 113 and *Eisenstadt v Baird* 405 U.S. 438).

[54] Article 4 of the International Covenant on Civil and Political Rights (ICCPR).

gradualism.[55] The CCPR General Comment No. 16 on Article 17 (Right to Privacy), recommends that information on the authorities and organs set up within the legal system of the State which are competent to authorize interference allowed by the law, and the laws and regulations that govern authorized interferences with private life be included in the State Parties' reports.[56]

Comparative Experience, International Standards and Best Practices

This section discusses the approaches to legislative protection of privacy in selected jurisdictions, with lessons and models for Sri Lanka to follow. It also sets out some international standards and best practices which would be useful to observe.

Experiences in countries where the right to privacy is constitutionally protected demonstrate that the mere existence of the right to privacy as a constitutionally protected right does not translate into effective protection of the right to privacy in practice. For instance, although the constitution of Uganda protects the right to privacy as a fundamental right, there are numerous instances where privacy is violated. On the other hand, it has been demonstrated that the presence of legislation on data protection without a constitutionally protected right to privacy is also inadequate. In Malaysia, the Personal Data Protection Act of 2010 protects the personal data of individuals but there is no constitutional right to privacy. It has been emphasized that data privacy does not encompass all aspects of privacy. A recent study ranked Malaysia among the five worst countries for privacy due to the rise in use of facial recognition technology, biometric identification, CCTV monitoring and intergovernmental agency data sharing without consent.[57]

---

[55] The Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights <https://www.icj.org/wp-content/uploads/1984/07/Siracusa-principles-ICCPR-legal-submission-1985-eng.pdf> accessed 19 August 2020.

[56] UN Human Rights Committee (HRC), CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, 8 April 1988, available at <https://www.refworld.org/docid/453883f922.html> [accessed 19 August 2020].

[57] A Tang, 'Study: Malaysia the fifth-worst country for personal data protection' (*The Star :Malaysia News*, 16 October 2019) <https://www.thestar.com.my/news/nation/2019/10/16/study-malaysia-the-fifth-worst-country-for-personal-data-protection> accessed 8 July 2020.

Prominent legal practitioners and others have highlighted the urgent need for a Privacy Act in Malaysia to effectively address these threats to privacy.[58]

Section 37 of Nigeria's 1999 Constitution forms the foundation of data privacy rights and protection in Nigeria. Section 37 guarantees and protects the right of Nigerians to privacy with respect to their homes, correspondence, telephone conversations and telegraphic communications. It deems privacy a fundamental right which is enforceable in a court of law when breached. Prior to the Nigeria Data Protection Regulations (NDPR) introduced in 2019, most cases of data privacy breaches were enforced under this section. The NDPR was issued by the National Information Technology Development Agency (NITDA) to comprehensively regulate and control the use of personal data in Nigeria. Apart from these, Nigeria has a several privacy enabled legislation in a variety of sectors such as health, child protection, consumer protection and telecommunications, creating a comprehensive and useful privacy legal framework.[59] This demonstrates that the most effective legal framework to adopt would be the constitutional protection of the right to privacy along with data protection legislation and other privacy enabled legislation.

Article 12 of the Universal Declaration of Human Rights of 1948 and Article 17 of the International Covenant on Civil and Political Rights of 1966 guarantee the right to privacy and protection of this right by law. Additionally, Article 16 of the Convention on the Rights of the Child of 1989 guarantees the right to privacy of children and protection of this right by law.

---

[58] S Buang, 'Urgent need for a privacy act' (*New Straits Times*, 1 March 2019) <https://www.nst.com.my/opinion/columnists/2019/03/465152/urgent-need-privacy-act> accessed 10 July 2020.

[59] O Babalola, 'Nigeria: Data Protection and Privacy Challenges in Nigeria (Legal Issues)' (*Mondaq*, 9 March 2020) <https://www.mondaq.com/nigeria/data-protection/901494/data-protection-and-privacy-challenges-in-nigeria-legal-issues-> accessed 13 July 2020. ; DLA Piper, 'Nigeria' (*DATA PROTECTION LAWS OF THE WORLD*, 20 May 2019 <https://www.dlapiperdataprotection.com/index.html?t=law&c=NG> accessed 14 July 2020.

The core OECD privacy principles adopted by the OECD Council in 1980 form the basis of many privacy legislation and could be adopted for Sri Lanka.[60]

It has been suggested that the government of Sri Lanka should bring necessary legislation with an institutional framework similar to the Right to Information Commission to effectively protect citizens' privacy, allowing the institution to act independently. Additionally, both the sub-committee on fundamental rights and on the independence of the judiciary recommended that the fundamental rights jurisdiction be given to lower courts. This would make it easier for citizens to access courts for remedies in cases of violations of fundamental rights.[61]

The Centre for Policy Alternatives (CPA) has consistently maintained that in order to ensure effective implementation, all law, policy, practice, and conduct inconsistent with the right to privacy (and more broadly with other Fundamental Rights as well as the whole of the constitution) must be made subject to judicial review and other public law remedies, including the devolution of judicial power so that Provincial High Courts become the courts of first instance for fundamental rights applications.[62] Most recently, in May 2020, in its submission to the United Nations General Assembly on Eliminating Intolerance and Discrimination Based on Religion or Belief, the CPA called attention to the absence of right to privacy in the ICCPR Act of Sri Lanka.[63]

---

[60]Organisation for Economic Co-Operation and Development, 'OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data' (*Organisation for Economic Co-operation and Development*, 2013) <https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm> accessed 14 July 2020.

[61] Fonseka, B., Ganeshathasan, L. and Daniel, S., 2017. *Two Years in Government: A Review of the Pledges Made In 2015 through the Lens of Constitutional Reform, Governance and Transitional Justice*. Centre for Policy Alternatives. Available at: <https://www.cpalanka.org/wp-content/uploads/2017/02/2-February-2017-FINAL-REPORT-.pdf> [Accessed 20 July 2020].

[62] Centre for Policy Alternatives, Preliminary Submission by the Centre for Policy Alternatives (CPA) to the Public Representation Commission (2016).

[63] Centre for Policy Alternatives, 'Report to the United Nations General Assembly on Eliminating Intolerance and Discrimination Based on Religion or Belief and the Achievement of Sustainable Development Goal 16 (SDG 16)'. Submission by the Centre for Policy Alternatives (CPA), Sri Lanka, May 2020.

Additionally, the lack of conditions such as 'necessity', 'reasonableness' or 'justifiability' in Article 15 of the Sri Lankan constitution has provided the state unwarranted space to 'legally' restrict Fundamental Rights. The vague and abstract interests including 'national economy', 'racial and religious harmony' and 'the general welfare of a democratic society' are overbroad and subject to possible abuse.[64]

[64] G. Gunatilleke, 2016. *A Rights-Based Approach to Limitation Clauses in the Sri Lankan Constitution: CPA Working Papers on Constitutional Reform No. 9*. Centre for Policy Alternatives. Available at: < https://www.cpalanka.org/wp-content/uploads/2016/11/Working-Paper-9.pdf> [Accessed 20 July 2020].

IV. The Right to Privacy in Sri Lanka

The need for the right to privacy has gained increased importance in Sri Lanka in light of recent policy reforms and legislative and administrative changes which are forthcoming. The following section examines the legislation, policies and perceptions surrounding the right to privacy in Sri Lanka.

The right to privacy was recommended to be included in the chapter on Fundamental Rights proposed for the new constitution of 2015.[65] More recently, strong privacy measures with regard to data protection are proposed[66] to be introduced through the draft Data Protection Act. While all these measures to protect privacy remain in the draft stage, the right to privacy continues to be violated and trivialized by the State as well as various non-state actors.

Even if the proposed Data Protection Bill becomes law, concerns surrounding the right to privacy will not be satisfactorily addressed, as informational privacy is only one aspect of privacy.[67]

This section highlights the absence of strong privacy protections in Sri Lankan legislation, proposed legislative and administrative reforms putting privacy further at risk and the consistent violation of privacy by various actors strengthened by the perception of privacy as an individual right to be set off against the common good. It is essential to incorporate a justiciable right to privacy within the chapter on Fundamental Rights in order to address this situation effectually, as it would give the most useful legal remedy to a citizen whose privacy is violated.

---

[65] Public Representations Committee on Constitutional Reform, 'Report on Public Representations on Constitutional Reform', 2016.

[66] Ministry of Digital Infrastructure and Information Technology, Final Draft of the Data Protection Bill (2019). <http://www.mdiit.gov.lk/index.php/en/what-we-diliver/downloads/acts/download/23-acts/78-data-protection-bill-2019-09-20-final>;Bar Association of Sri Lanka, 2020. "*Connecting Through Digital Platforms, Data Protection and Cyber Security*". (Webinar). 25 July 2020.

[67] Bar Association of Sri Lanka, 2020. "*Connecting Through Digital Platforms, Data Protection and Cyber Security*". (Webinar). 25 July 2020.

The Constitutional Reform Project of 2015

This section will briefly examine the recent constitutional reform project and attempts to address the issue of the right to privacy. The strengthening of the Fundamental Rights chapter was promised as part of the constitutional reform project of 2015. The report of the sub-committee on Fundamental Rights recommended the recognition of several new rights, which included the right to privacy.[68] However, the public debate on the right to privacy was limited as some of the other aspects of the proposed constitutional reforms generated much controversy while others were wholly ignored.[69]

A 2016 survey conducted by the Faculty of Law of the University of Colombo among its undergraduates revealed that only 2% of the participants believed that the right to privacy should be introduced into the chapter on Fundamental Rights.[70] One of the main reasons for this apparent apathy about privacy protections is the lack of awareness among the general public about the importance of their privacy and personal information. Speaking to media recently, the Chairman of the Information Technology Society of Sri Lanka (ITSSL) said that owing to low digital literacy, people neither know about, nor pay attention to, their user rights and privacy.[71]

CPA in its submission to the Public Representations Committee on Constitutional Reforms (PRC) stated that the 'current chapter on fundamental rights falls short on a number of counts in meeting general international standards as well as Sri Lanka's international obligations'. In its submission, CPA recommended the introduction of a new bill of Fundamental Rights which would fully meet the standards set under

---

[68] Fonseka, B., Ganeshathasan, L. and Daniel, S., 2017. *Two Years in Government: A Review of the Pledges Made In 2015 through the Lens of Constitutional Reform, Governance and Transitional Justice*. Centre for Policy Alternatives. Available at: <https://www.cpalanka.org/wp-content/uploads/2017/02/2-February-2017-FINAL-REPORT-.pdf> [Accessed 20 July 2020].

[69] A Welikala, 'Constitutional Reforms in Sri Lanka – More Drift?' [2019] 108(6) The Round Table <DOI: 10.1080/00358533.2019.1687964> accessed 22 July 2020.

[70] Survey for submission to the Public Representations Committee for the drafting of a new Constitution for Sri Lanka. Available at <https://law.cmb.ac.lk/wp-content/uploads/2016/05/Survey-for-Submission-to-the-Public-Representations.pdf> accessed 22 July 2020.

[71] S Chamara, 'Do We Have the Right to Privacy?' *Ceylon Today* (Colombo) 26 January 2020 <https://archive.ceylontoday.lk/print-more/50553> accessed 24 August 2020.

the core international human rights instruments recognised by the United Nations. This would have included the right to privacy as guaranteed by the International Covenant on Civil and Political Rights, and the Universal Declaration on Human Rights.

Further, the Report of the Public Representations Committee on Constitutional Reforms recommended the recognition of the right to privacy as a fundamental right of all persons.[72] The right to privacy would include the right to be protected from arbitrary interference with family life, the inviolability of the home, correspondence and communication and being subjected to unlawful attacks on a person's honour and reputation.[73]

However, due to lack of political will as well as polarizations within the Sri Lankan community in their perceptions of the constitutional reform project, the proposed new constitution was never adopted.[74] With the change in government in 2019 and the electoral victory in August 2020, the focus of proposed constitutional amendments has significantly changed with the likelihood of changes to the pro-democracy reforms introduced in 2015.[75]

---

[72] Public Representations Committee on Constitutional Reform, 'Report on Public Representations on Constitutional Reform', 2016. At pg 97.

[73] The right to privacy was recommended with special reference to the rights of people with diverse sexual and gender identities. In this context, the report also called for the repeal of Articles 363 and 365A of the Penal Code and the Vagrants Ordinance, which violate the privacy of members of the LGBTQ+ community leading to discrimination against them. The right of all persons of full age, without any limitation due to race, nationality or religion, gender identity or gender and sexual orientation to marry and to found a family was also recognized, with equal rights as to marriage, during marriage and its dissolution. The right to privacy was also specified along with its implications for persons with disabilities. This would include protection from interference and surveillance of medical and other records, correspondence and any other type of otherwise private communication, including in the home and family as well as in the electoral process.

[74] A Welikala, 'Sri Lanka's (un)ending road to a new Constitution: Technical progress, political collapse' (*Constitutionnet*, 29 January 2020) <http://constitutionnet.org/news/sri-lankas-unending-road-new-constitution-technical-progress-political-collapse> accessed 24 August 2020.

[75] Economy Next, 'Sub-committee to draft 20th amendment to Sri Lanka constitution; 19A out, salient features to remain' *Economy Next* (Colombo) 20 August 2020 < https://economynext.com/sub-committee-to-draft-20th-amendment-to-sri-lanka-constitution-19a-out-salient-features-to-remain-73210/> accessed 24 August 2020. ; The Indian Express, 'Sri Lankan President Gotabaya Rajapaksa vows to abolish 19th Amendment' *The Indian Express* (Mumbai) 20 August 2020

Sri Lanka has made several attempts at constitutional reform over the years. For example, the 2000 draft Constitution which was certified by the Cabinet of Ministers as a Bill and was intended to be passed by the Parliament also recognized the right to private and family life but this too never materialised.[76] Considering the political context, it is unlikely that we would see constitutional and legislative reforms introduced that will fully embrace the principle of the right to privacy in the near future.

Current Legal Framework in Sri Lanka

As at present, there is no clear legal remedy available for the violation of the privacy of an individual. Although Sri Lanka has ratified the International Covenant on Civil and Political Rights (ICCPR), the ICCPR Act which incorporates the Covenant into domestic law misses several key Articles of the Covenant, including the right to privacy. Although the right to privacy is amongst Sri Lanka's international human rights obligations, this is not reflected in domestic law.[77]

The ICCPR Act is based on the premise that the existing legal framework in Sri Lanka substantially protects the rights recognised by the ICCPR.[78] This position was endorsed by the Supreme Court in its ICCPR Advisory Opinion of 2008. The right to privacy is established by Article 17 of the ICCPR. In its Advisory Opinion, the Supreme Court stated that various common law private law rights and subject specific statutory provisions already protect the right to privacy in Sri Lanka.

<https://indianexpress.com/article/world/sri-lankan-president-gotabaya-rajapaksa-vows-to-abolish-19th-amendment-6563179 > accessed 24 August 2020.

[76] The Draft Constitution of Sri Lanka, August 03, 2000. <http://confinder.richmond.edu/admin/docs/srilanka_constitution.pdf> ; J Wickramaratne, 'Constitutional Reform In Sri Lanka: Issues And Prospects' (London) Amirthalingam Memorial Oration, 12 July 2014. Available at < https://www.colombotelegraph.com/index.php/constitutional-reform-in-sri-lanka-issues-and-prospects/> accessed 24 August 2020.

[77] As per the CCPR General Comment No. 16: Article 17 (Right to Privacy), the obligations imposed by this article require the State to adopt legislative and other measures to give effect to the prohibition against such interferences and attacks as well as to the protection of this right.

[78] International Covenant on Civil and Political Rights (ICCPR) Act, No. 56 of 2007. [Certified on 16th November, 2007]. See long title and preamble of the Act.

However, neither the Constitution nor the ICCPR Act protect the right to privacy as a fundamental human right.[79]

ICCPR	Annexure to the ICCPR Advisory Opinion
Article 17	Common law delictual right to sue for damages loss of reputation
	Post Office Ordinance, No. 11 of 1908: Sections 71, 75
	Computer Crimes Act, No 24 of 2007: Sections 3, 8, 10

Figure 1: From the Annexure to the Supreme Court's Advisory Opinion of 2008

The existing case law on privacy is limited to the use of the Roman Dutch law action of *actio iniuriarum* to protect the right to privacy and dignity against defamatory action or content. The Post Office Ordinance contains several provisions penalizing violations of privacy by opening mail by officers of the post office or others without legal authority. Under section 56 of the Ordinance, any officer of the post office requires an order in writing from the Minister or the direction of a competent court in order to open any postal article.

Under section 75, it is an offence to disclose the contents of a postal article opened under the authority of this Ordinance, except so far as may be necessary for the purpose of returning the same or so far as may be authorized by the Postmaster-General in writing.

Under section 74, only a person who is the parent or guardian of a minor or a ward may open letters addressed to such minor or ward. Opening letters addressed to another person under any other circumstances is an offence under the Ordinance punishable by imprisonment and/or fine.[80]

However, these provisions are extremely inadequate to address breaches of privacy created by sophisticated technological interventions. In light of the fact that most personal communications are carried out using virtual media, the privacy

[79] This position was maintained by CPA as an intervenient-petitioner in SC Ref no. 01/2008. Centre for policy alternatives, 'The Centre for Policy Alternatives Vs Attorney General (SC Ref: No1/2008)' (*Public Interest Litigation Submissions*, 2 November 2008) <https://www.cpalanka.org/the-centre-for-policy-alternatives-vs-attorney-general-sc-ref-no-12008/> accessed 23 July 2020.

[80] Post Office Ordinance, No. 11 of 1908.

protections guaranteed by the Post Office Ordinance are largely irrelevant to the wider concerns surrounding privacy in Sri Lanka.

The Computer Crimes Act makes provision for the protection of privacy in a few instances. Under section 3, securing unauthorised access to a computer is an offence. Under section 8, the illegal interception of data is an offence. Unauthorised disclosure of information enabling access to a service is an offence under section 10. All of the above offences are punishable by imprisonment and/or fine. However, the same Act creates a potential privacy threat. Section 18 of the Act confers the power to an expert or a police officer involved in an investigation under the Act to tap any "wire or electronic communication" or obtain any information (including subscriber information and traffic data) from any service provider. The provision includes the "safeguard" of obtaining the authority of a warrant from a magistrate for this purpose but, given that warrants are available for the asking (and no warrant is required in a case of urgency), this gives rise to a serious threat to privacy.[81] A police officer may also seize electronic equipment and devices under section 22 of the Act.[82]

In addition to the above Acts referred to in the Advisory Opinion, Chapter 32 of the Intellectual Property Act of 2003 makes provision for the protection of undisclosed information and trade secrets which could be used for unfair commercial advantage.

It is evident that the existing privacy enabled legislation referred to in the Supreme Court's Advisory Opinion is subject specific and inadequate to protect all aspects of privacy. Moreover, the ICCPR envisions the protection of the right to privacy as a human right in addition to other private law remedies which may protect privacy in specific situations.[83]

---

[81] A Marsoof, 'The Right to Privacy in the Information Era: A South Asian Perspective [2008] 5(3) SCRIPTed - A Journal of Law, Technology & Society <http://ssrn.com/abstract=1578222> accessed 22 June 2020.

[82] Computer Crimes Act, No 24 of 2007.

[83] Edrisinha, R. and Welikala, A. 2016. *Civil and Political Rights in the Sri Lankan Constitution and Law: Making the New Constitution in Compliance with the ICCPR: CPA Working Papers on Constitutional Reform No. 8*. Centre for Policy Alternatives. Available at: <https://www.cpalanka.org/wp-content/uploads/2016/11/Working-Paper-8.pdf> [Accessed 20 July 2020].

In fact, there are several legal provisions which directly threaten the privacy of individuals. The Sri Lanka Telecommunications Act gives a telecommunications officer the power to intercept communications under the direction of a minister, which creates fears about privacy and surveillance of personal communications by the State.[84] The order of a competent court is not required to intercept personal communications under the Act, raising concerns about arbitrariness and rule of law. At present, the Ministry under which the Telecommunications Regulatory Commission of Sri Lanka comes is not clear, creating a responsibility and accountability gap.

Further, the existence of colonial era laws criminalizing consensual sexual activity between adults in sections 363 and 365A of the Penal Code violates the right to privacy. Additionally, the Vagrants Ordinance is also used to violate the privacy of marginalized groups. The Report of the Public Representations Committee on Constitutional Reforms recommends the repeal of these provisions in the Penal Code and the Vagrants Ordinance.[85]

The Nineteenth Amendment to the Constitution introduced the right to information as a Fundamental Right. The Right to Information Act and the institutional framework introduced under the Act ensures that the public can access information about decisions which affect them and that these decision-making processes remain transparent. Both Article 14A and the Right to Information Act restrict the right to information in the interests of privacy or for preventing the disclosure of information communicated in confidence. However, under section 5(1) (a) of the Right to Information Act, privacy is subject to the larger public interest of the disclosure of such information.

It must be noted that Sri Lanka does not yet have data protection legislation. Thus, the constitutional protection of the right to privacy is essential to balance the right to

[84] See sections 53 and 54 of Sri Lanka Telecommunications Act, No. 25 of 1991.
[85] Public Representations Committee on Constitutional Reform, 'Report on Public Representations on Constitutional Reform', 2016 at pg 114.

information and the right to privacy to ensure that both rights are exercised meaningfully.

Proposed Legislation on Data Protection

In a context where the right to privacy is not included in the fundamental rights chapter of the Constitution of Sri Lanka, special attention is required with regard to legal provisions on data protection including proposals in this area. This need is compounded with the right to privacy being increasingly violated by the development of new technologies allowing online surveillance by companies and governments. While the Government of Sri Lanka is in the process of drafting[86] a Data Protection Act, its adequacy and effectiveness in practice remains to be seen. Concerns remain including the change in convictions and behaviours of business entities collecting and processing personal data to ensure that the draft Act is implemented effectively.[87]

The drafting of the proposed data protection legislation was initiated following a request made by the Central Bank of Sri Lanka (CBSL) in 2018, as data protection legislation was crucial to attracting foreign direct investment (FDI) and increasing cross border e-commerce activities. One must note that compliance with international standards in data protection is necessary and will benefit Sri Lanka in carrying out international business activities. Data protection regulations such as the General Data Protection Regulation (GDPR) in Europe are virtually borderless in their application. They extend to any entity, irrespective of their jurisdiction, as long as they take data from Europe. As such, a corporate culture embracing strict privacy and data protection principles is necessary to establish the trust of customers and

[86] International Association of Privacy Professionals, 'Final draft of Personal Data Protection Bill introduced in Sri Lanka' *IAPP*, 10 October 2019 <https://iapp.org/news/a/final-draft-of-personal-data-protection-bill-introduced-in-sri-lanka/> accessed 27 July 2020. ; Daily FT, ''Data is the new oil': An introduction to the proposed Data Protection Act' *Daily FT* (Colombo) 6 December 2019 < http://www.ft.lk/columns/Data-is-the-new-oil-An-introduction-to-the-proposed-Data-Protection-Act/4-691056> accessed 27 July 2020.

[87] For instance, the awareness of business entities that collection and possession of personal data increases their liability in terms of expenses and effort to secure the data and attaches legal responsibility in case of a breach.

partners locally and overseas, giving economic opportunities to Sri Lankan entrepreneurs.

According to the draft Data Protection Act[88], Personal Data is "any information that can identify a data subject directly or indirectly, by reference to-

1. an identifier such as a name, an identification number, location data or an online identifier, or
2. one or more factors specific to the physical, physiological, genetic, psychological, economic, cultural or social identity of that individual or natural person.[89]"

There is also an increasing reliance on digital and cloud services which collect data in Sri Lanka. For example, transportation applications such as Uber and PickMe both collect data for offline analysis. There is increased usage of social media platforms and cloud communication platforms for email and calendar management (e.g. Google mail and calendar). These systems, being the primary means of communication, collect large amounts of data daily and then target advertisements based on these collected data.[90]

The use of Virtual Private Networks (VPN) also brings in data security concerns. In certain cases, applications providing this service for free, sell consumer internet activity data to advertisement targeting agencies. Given the fact that VPNs can capture all data that are being transmitted or received by a device, the information captured can be very detailed (e.g. unencrypted messaging services, location, contact information, application usage) and can easily be personally identifiable.

At present, Sri Lanka does not have a cross-sectoral data protection law. There are several data protection enabled legislation such as the Banking Act No. 30 of 1988,

[88] Ministry of Digital Infrastructure and Information Technology, Final Draft of the Data Protection Bill (2019). <http://www.mdiit.gov.lk/index.php/en/what-we-diliver/downloads/acts/download/23-acts/78-data-protection-bill-2019-09-20-final>

[89] Section 46 of the draft Act. Ministry of Digital Infrastructure and Information Technology, Final Draft of the Data Protection Bill (2019). <http://www.mdiit.gov.lk/index.php/en/what-we-diliver/downloads/acts/download/23-acts/78-data-protection-bill-2019-09-20-final>

[90] This paper only comments on the legal dimensions of the right to privacy as affected by various practices and is not an exhaustive study of the collection and use of personal data.

Sri Lanka Telecommunications Act No. 25 of 1991, Intellectual Property Act No. 36 of 2003, Computer Crimes Act No. 24 of 2007, and Registration of Persons (Amendment) Act No. 8 of 2016. The proposed Data Protection Act, if enacted, would provide a legal framework extending to both the State and private sectors.

In January 2020, then subject Minister, Bandula Gunawardana, said that the proposed Data Protection Act does not come under his Ministry and that it had been transferred to the Ministry of Defence following the change of government.[91]

Following the change of government in 2019, most of the digital security subjects and institutions such as the Telecommunications Regulatory Commission of Sri Lanka (TRCSL), Information and Communication Technology Agency (ICTA) and Sri Lanka Computer Emergency Readiness Team (SLCERT) were transferred to the Ministry of Defence. The Information and Communication Technology Act, Sri Lanka Telecommunications Act and the Electronic Transactions Act fall within the Minister of Defence. It is unclear whether they remain under the Ministry of Defence following the delineation of duties of Ministers set out in Gazette Extraordinary No. 2187/27 of 09 August 2020. If these subjects are under the purview of the Minister of Defence, it raises concerns of uncertainty and lack of accountability, as there is no Minister of Defence appointed by the President, at the time of writing this paper.[92] This is particularly worrying in light of the increased militarization and securitization of the state, including the appointment of retired military personnel to head the TRCSL and ICTA.[93]

[91] The Morning, 'Data Protection Bill further delayed' *The Morning* (Colombo) 19 January 2020 < http://www.themorning.lk/data-protection-bill-further-delayed/> accessed 30 July 2020.

[92] Gazette Extraordinary No. 2188/42 of 13 August 2020.

[93] Centre for Policy Alternatives, 'Sri Lanka's Recent Political Challenges & Prospects for the Future' (March 2020) available at < https://www.cpalanka.org/sri-lankas-recent-political-challenges-prospects-for-the-future/> accessed 27 July 2020.

As per the draft Act, the data subject shall be entitled to request in writing for rectification or completion of any inaccurate or incomplete personal data, erasure/deletion of the personal data, or withdrawing consent for the processing of personal data.

The data subject shall have a right to request a controller to review a decision based solely on automated processing and affecting his/her rights and freedoms as guaranteed under any written law.[1] The previous draft included broader principles, such as 'legitimate interests', 'rights' and 'freedoms', which have now been removed.

In cases where the processing of personal data is "likely to result in a high risk to the rights and freedoms of data subjects", a controller has to carry out a privacy impact assessment prior to such processing.[1]
The final draft of the Act enables data subjects to claim their aforementioned rights by directly approaching the controller of the personal data. The controller now has to inform the data subject about their right of appeal in cases where the controller refuses or restricts the rights of data subjects. This obligation is an improvement on the previous draft.

A clause in the final draft of the Act provides certain exceptions to the protection of personal data for "essential objectives of general public interest". [1] It is suggested that this exception is framed too widely.

The obligations of a [data] controller as per Part II of the draft Act may be outlined as follows:

1. Section 5 – Obligation to process personal data in a lawful manner
2. Section 6 – Obligation to define a purpose for processing
3. Section 7 – Obligation to confine processing to the defined purpose
4. Section 8 – Obligation to ensure accuracy
5. Section 9 – Obligation to limit the period of retention
6. Section 10 – Obligation to maintain integrity and confidentiality
7. Section 11 – Obligation to process personal data in a transparent manner
8. Section 12 – Accountability in the processing of personal data

Every controller, unless exempted from this Act or any written law, has to appoint a 'Data Protection Officer' ('DPO') to ensure compliance with the Act. A DPO will be a senior staff member of the controller with relevant academic or professional qualifications in matters relating to data protection.[94]

The previous draft included provisions for the mandatory registration of controllers. However, this has been removed in the final draft. Instead, the accountability obligations require controllers to implement internal controls and procedures, known as a 'Data Protection Management Programme'.[95]

Part V of the draft Act provides for the designation "of [a] Public Corporation, Statutory Body or any other institution (…) as the 'Data Protection Authority'.

The drafting of legislation

The drafting of legislation is carried out by the Legal Draftsman's Department. Once the draft is sent to the Cabinet of Ministers and receives Cabinet approval, it is published in the Gazette.[96] Upon the lapse of two weeks from the date the Bill was gazetted, the government can table the Bill in Parliament at any time. Once the Bill is placed on the Order Paper of the Parliament it is open to any citizen to challenge

[94] Section 20 of the draft Act. Ministry of Digital Infrastructure and Information Technology, Final Draft of the Data Protection Bill (2019). <http://www.mdiit.gov.lk/index.php/en/what-we-diliver/downloads/acts/download/23-acts/78-data-protection-bill-2019-09-20-final>

[95] Section 12 of the draft Act. Ministry of Digital Infrastructure and Information Technology, Final Draft of the Data Protection Bill (2019). <http://www.mdiit.gov.lk/index.php/en/what-we-diliver/downloads/acts/download/23-acts/78-data-protection-bill-2019-09-20-final>

[96] Article 78 of the Constitution of the Democratic Socialist Republic of Sri Lanka (as amended).

such Bill in the Supreme Court within a period of one week.[97] No proceedings can be had in relation to such Bill in Parliament until the determination of the Supreme Court is forwarded to the Speaker. Concerns have already been raised re the setbacks with Sri Lanka's law-making process including the limited time where a Bill can be challenged. Additionally, there is no transparency or participation in the process of drafting legislation. In the instance of the proposed Data Protection Act, the draft was released to the public through the website of the Ministry of Digital Infrastructure and Information Technology and was modified after consultations with relevant stakeholders. However, wider discussion and debate among the general public should be generated to ensure as wide a participation as possible and with it, greater awareness among the public as to potential implications on their rights. As it is still in the draft stage any further amendments following changes in government policy must also be closely monitored. The drafting process must come under close observation by all stakeholders and comments offered through consultation processes where possible.

National Security and the Right to Privacy

Sri Lanka has a history of disregarding human rights in emergency situations, especially in the perceived interest of national security. Due to the absence of constitutional and legislative protection of the right to privacy, it has been violated with impunity. This was evidenced during the war and the post war period and has renewed relevance in the present context as the current president was elected in November 2019 on a national security and securitization campaign platform.

This section discusses executive action which violates or poses a potential threat to the right to privacy in the name of national security, including practices which were put in place during the war which continue to have consequences even today as well as recent reforms proposed in the name of strengthening national security.

The violation of the right to privacy was a matter of serious concern during the war, given that intelligence and other covert operations were often conducted extra-

[97] Article 121 of the Constitution of the Democratic Socialist Republic of Sri Lanka (as amended).

legally, and without any judicial protection being afforded against the arbitrary use of power.[98] Moreover, cordon and search operations and *en masse* detentions were common, purportedly in the exercise of emergency powers and/or anti-terrorism legislation, having the effect of discriminatory treatment and violation of the fundamental rights of ethnic minorities and critics of the government.[99] A constitutional right to privacy might have provided an avenue for a judicial protection to prevent such arbitrary action in the guise of national security.[100]

Privacy is also violated by arbitrary executive action with regard to interception of personal communications without due process or a clear legal basis, and surveillance of public social media activities by intelligence services to identify 'those who could be a threat to national security'. For example, in 2014, during a parliamentary debate on the right to privacy, MP Wickramaratna alleged that there are some telecommunication companies that were passing on people's personal information to the Defence Ministry which was in violation of international law. "However much these companies come under duress from the Defence authorities, they cannot divulge people's personal information to State authorities," he said, adding that he would reveal the names of these companies when necessary.[101]

Another practice which infringes the right to privacy ostensibly introduced to protect the interests of national security is the licensing of news websites by the Telecommunications Regulatory Commission (TRC). Section 17 of the Sri Lanka

---

[98] United Nations Human Rights, Office of the High Commissioner, (September 2015) 'Report of the OHCHR Investigation on Sri Lanka (OISL)' Available at <https://www.ohchr.org/EN/HRBodies/HRC/Pages/OISL.aspx> accessed 24 August 2020.

[99] United Nations Human Rights, Office of the High Commissioner, Info Note 3, Report of the OHCHR Investigation on Sri Lanka, (September 2015) 'Violations related to deprivation of liberty and enforced disappearances'. Available at <https://www.ohchr.org/EN/HRBodies/HRC/Pages/OISL.aspx> accessed 24 August 2020.

[100] Edrisinha, R. and Welikala, A. 2016. *Civil and Political Rights in the Sri Lankan Constitution and Law: Making the New Constitution in Compliance with the ICCPR: CPA Working Papers on Constitutional Reform No. 8*. Centre for Policy Alternatives. Available at: <https://www.cpalanka.org/wp-content/uploads/2016/11/Working-Paper-8.pdf> [Accessed 20 July 2020].

[101] Kirinde, C., 'Govt. plays Peeping Tom with its proposed eNIC' *The Sunday Times* (Colombo) 24 August 2014 <http://www.sundaytimes.lk/140824/columns/govt-plays-peeping-tom-with-its-proposed-enic-114692.html>

Telecommunications Act states that no person shall operate a telecommunication system in Sri Lanka without a license.

A "telecommunication system" is defined in Section 73 as,

> *"a system for the conveyance by the agency of electric, magnetic, electro-magnetic, optic, electro-chemical or electromechanical energy, of*
> *a) speech, music and other sounds*
> *b) visual Images;*
> *c) information for human comprehension that is intended for presentation in a two-dimensional form, consisting of symbols, phrases or sentences in natural or artificial languages, pictures, diagrams and tables; or*
> *d) signals serving for the actuation or control of machinery or apparatus."*

A news website may be accessed using a telecommunication system licensed under the Act but a news website itself is not a telecommunication system requiring to be licensed. Thus, it is not clear how the TRC derives the authority to license news websites, requiring extensive information on these websites which could potentially violate the right to privacy while stifling the freedom of expression. This is especially a cause for concern considering the history of intimidation and violence unleashed on opponents and critics of government action by successive governments.[102]

Recent research has cast doubt on the perceived dichotomy of 'privacy vs. security', and suggested the possibility that data gathering and surveillance could harm both privacy and security. It has been argued[103] that where excessive 'security' measures are brought in they can lower the level of trust and, as a consequence, lower levels of cooperation with authorities, which again could damage rather than help security. The idea that 'tightening' security actually improves security is one that should not be taken at face value.[104]

---

[102] R Samarajiva, 'Quo warranto, TRC?' (*LIRNEasia*, 14 February 2010) <https://lirneasia.net/2010/02/quo-warranto-trc/> accessed 24 July 2020.
[103] P Bernal, 'Data gathering, surveillance and human rights: recasting the debate' [2016] 1(2) Journal of Cyber Policy <DOI: 10.1080/23738871.2016.1228990> accessed 24 July 2020.
[104] ibid.

A study[105] on the social integration of former LTTE combatants demonstrates that one of the primary reasons for their continued social isolation is the sophisticated culture of surveillance pervading the former war zones of Sri Lanka. While this surveillance structure may be justified by some from a national security point of view, it in fact greatly impedes the reintegration of ex-LTTE combatants and any sense of social cohesion. Many former combatants are constantly watched, followed, and called in for hours of questioning during which they are asked the same questions they have answered many times before, instilling in them a sense of fear and a sense that they are under constant surveillance. Interviews with former combatants show that, aware of the dangers, they self-regulate and 'discipline' themselves accordingly. The continued security apparatus that exists in the North and East of the country further adds to this culture of surveillance. The long-term individual and social costs of this loss of privacy are yet to be seen.[106]

Counterterrorism legislation also poses a threat to the right to privacy in Sri Lanka. The offence of failure to give information set out in both the Prevention of Terrorism Act (PTA) and the draft Counter Terrorism Act (CTA) has the potential to be abused unless carefully interpreted so as to prevent violating the liberties of persons, especially the right to privacy.[107] Additionally, while the PTA limited the powers of search and seizure only to police officers not below the rank of Superintendent or any other police officer, not below the rank of Sub-Inspector authorized in writing by him, the proposed CTA empowers any police officer to exercise these powers. This could potentially violate the right to privacy further. However, with reference to arrest, the CTA specifies that an arrest shall be carried out with due regard to privacy, which is in keeping with international law and best practices.[108] The CTA

[105] A Amarasingam, 'Life in the Open-Air Panopticon: Surveillance and the Social Isolation of Ex-LTTE Combatants in Sri Lanka' (*Groundviews*, 20 May 2014) <https://groundviews.org/2014/05/20/life-in-the-open-air-panopticon-surveillance-and-the-social-isolation-of-ex-ltte-combatants-in-sri-lanka/> accessed 24 July 2020.

[106] ibid.

[107] Centre for Policy Alternatives, 'Comparing the Proposed Counter Terrorism Bill to the Prevention of Terrorism Act' (October 2018) available at <https://www.cpalanka.org/wpcontent/uploads/2018/10/CTAPTA_final-.pdf> accessed 27 July 2020.

[108] ibid.

also makes provision for obtaining information from banks, financial institutions, telecommunication, satellite or digital service or data service providers, and government or statutory institutions which could be exploited in a manner that is invasive of the right to privacy of citizens and organizations.[109]

Recent policy reforms suggest that this surveillance apparatus established in the name of national security has the potential to encroach on the digital sphere. The Secretary of Defence Maj. Gen. (Retd) Kamal Gunaratne addressing members of the Information and Communication Technology Agency (ICTA) said,

> *"The motive behind placing (ICTA) under the Defence Ministry's purview is to pursue and facilitate the process. In the absence of national security ICT is of no use. It is a privilege for you to be under the Defence Ministry because the Ministry has more access, more power and more resources."*

He further said that the government is to digitise the entire State mechanism under an integrated system under the supervision and management of the Information and Communication Technology Agency (ICTA).[110]

On 14 January 2020, the Cabinet approved the proposal to draft a National Intelligence Act.[111] It was stated that the work and recommendations for reform made by the intelligence apparatus has been very useful in addressing threats to national security. However, their activities were reportedly restricted as there is no legislation empowering them. The proposed Act will cover all areas of intelligence and authorise extensive action by intelligence agencies. There is no further information publicly available on this proposed Act at the time of writing this paper.

[109] ibid.
[110] Ministry of Defence, 'Govt. to digitalise and integrate entire government machinery' (Press Release) 24 January 2020. <http://www.defence.lk/Article/view_article/841> accessed 24 July 2020.
[111] Ministry of Defence, 'Govt. gives green light to draft new National Intelligence Act' (Press Release) 16 January 2020. <http://www.defence.lk/Article/view_article/829> accessed 24 July 2020.

In February 2020, the report of the Sectoral Oversight Committee on National Security was released.[112] This report proposes the creation of a Central Data Centre under the Telecommunications Regulatory Commission to access the data of customers obtaining SIM cards. It also asserts[113] that "about two percent of the total Muslim population of the country are bent towards extremist ideologies. Considering that this could constitute a dire threat to the national security, such groups should be made to undergo a de-radicalization process under the aegis of the Ministry of Defence and with inputs from psychologists." The Sectoral Oversight Committee recommends surveillance using community as well as social media activities of persons to identify such 'radicalized personnel'.[114]

Further, public reports have documented the use of surveillance that have implications for an individual's right to privacy. For example, testifying before the Presidential Commission of Inquiry probing Easter Sunday attacks, former State Intelligence Service (SIS) Director SDIG Nilantha Jayawardena said that SIS had reported 'an unusual increase' in Muslim students at the Law College in 2012.[115] The racial/religious profiling of students by SIS poses a threat to the privacy of students and encroaches upon a host of other fundamental rights such as the right to equality and freedom of religious belief.

According to the report of the Select Committee of Parliament to look into and report to Parliament on the Terrorist Attacks that took place in different places in Sri Lanka

---

[112] C Kirinde, 'Parliamentary Committee calls for suspension for ethnic, religion-based parties' *Daily FT* (Colombo) 25 February 2020 < http://www.ft.lk/front-page/Parliamentary-Committee-calls-for-suspension-for-ethnic-religion-based-parties/44-696340> accessed 27 July 2020.

[113] The report does not cite any sources for this assertion, merely referring to 'expert view,' a vague term which is not further explained in the report.

[114] The Parliament of Sri Lanka, 'Report of the Sectoral Oversight Committee on National Security', 19 February 2020. <https://www.parliament.lk/uploads/comreports/1582610584075624.pdf#page=1> ; In a recent video conference organized by the Ministry of Foreign Relations to discuss 'strategic communications', a Sri Lankan diplomat suggested that an anti-terrorism task force on cyber security should be established to monitor social media platforms of youth in Europe, especially Sri Lankan Tamil individuals living in the area.

[115] A. Marsoof, 'Education and Employment, No Longer a Right of the Minorities?' (*People's Rights Group*, 31 July 2020) < https://www.prgsrilanka.org/education-and-employment-no-longer-a-right-of-the-minorities/> accessed 4 August 2020.

on 21st April 2019, there are multiple intelligence groups carrying out surveillance activities in Sri Lanka.[116] The report raises concerns about the lack of expertise and training in intelligence gathering among key individuals responsible for this task as well as politicisation of security and intelligence sectors and recommends greater oversight over this intelligence framework.[117] However, the manner in which these intelligence activities are carried out at present could pose a potential threat to privacy.

Right to Privacy and Public Health (COVID-19 Response)

In April 2020, the Ministry of Health and Indigenous Medical Services issued guidelines[118] to the media on reporting on the COVID-19 pandemic, warning that stigmatising people who had contracted the virus could make them hide their condition. The guidelines prohibited mentioning the race or religion of persons infected with COVID-19 or of those who die of it and publishing of photographs or videos of those infected with COVID-19 without their consent.[119]

Further to these guidelines, the Department of Government Information issued some additional standards to be followed when reporting sensitive information with reference to COVID-19 patients and their families.[120] These guidelines recommended that media entities refrain from broadcasting footage of cremation of patients who died of COVID-19 in a way that would cause disrespect to them or reveal the identity of their family members.

---

[116] Report of the Select Committee of Parliament to look into and report to Parliament on the Terrorist Attacks that took place in different places in Sri Lanka on 21st April 2019. Available at < https://www.parliament.lk/uploads/comreports/sc-april-attacks-report-en.pdf> accessed 27 July 2020.

[117] B Fonseka, 'Is the Deep State Involved? Reflections on the PSC Findings & Implications for the Future' (*Groundviews*, 31 October 2010) < https://groundviews.org/2019/10/31/is-the-deep-state-involved-reflections-on-the-psc-findings-implication-for-the-future/> accessed 24 July 2020.

[118] Daily FT, 'Health Ministry issues guidelines on COVID-19 reporting' *Daily FT* (Colombo) 3 April 2020 <http://www.ft.lk/news/Health-Ministry-issues-guidelines-on-COVID-19-reporting/56-698459> accessed 27 July 2020.

[119] ibid.

[120] Department of Government Information, 'Standards for reporting sensitive information on COVID-19 patients and their families' 06 April 2020. < http://www.newswire.lk/2020/04/06/new-guidelines-issued-to-media-over-covering-covid-deaths-suspected-patients/> accessed 29 July 2020.

However, not all media entities have complied with the guidelines and standards. According to an analysis conducted by EthicsEye, from 6 April to 8 May 2020, based on weekday prime time new telecasts of selected Sinhala language TV channels, most of them had violated the guidelines.[121] Certain electronic and print media channels reveal the identity of confirmed patients or those quarantined due to contact with patients. Additionally, the use of problematic terms like 'corona suspects' have at times created panic and stigmatised the patients.

In April, the Ministry of Defence[122] also requested print and electronic media to respect the privacy of COVID-19 patients and to refrain from recording and airing footage of their homes being inspected by health workers. The Defence Ministry said in a statement that contact tracing and other pandemic related activities carried out by Public Health Inspectors (PHIs) and police officers have been featured in a number of news telecasts, other programmes and feature articles in newspapers.

It was emphasised that protecting patients' privacy is important to encourage patients to come forward for testing, and that covering such events would also cause inconvenience to health officials on duty.

In the wake of COVID-19, anti-Islamic sentiments and anti-Muslim hate has taken on a new form. Various media entities attempt to implicate the Muslim population, who make up 10% of Sri Lanka's multicultural population, of being 'super-spreaders' of the virus. This is not limited to journalists and editors, with even the country's leading trade union of medical doctors displaying anti-Islamic bias in giving professional advice to the government to racially profile the Muslim population.[123]

---

[121] In a recent development, in June 2020, Ethics Eye received a lawyer's letter of demand on behalf of a television news channel owner/manager, indicating that the news channel considered this analysis objectionable, and demanding a sum of Rs. 1 billion as damages and threatening court action if the sum demanded was not paid. The letter also threatened to restrain Ethics Eye from publishing the said posts in the future.

[122] Economy Next, 'Sri Lanka's defence ministry requests media to respect privacy of COVID-19 patients' *Economy Next* (Colombo) 28 April 2020 <https://economynext.com/sri-lankas-defence-ministry-requests-media-to-respect-privacy-of-covid-19-patients-68796/> accessed 24 August 2020.

[123] Daily FT, 'GMOA's COVID-19 exit strategy advocates racial profiling' *Daily FT* (Colombo) 18 April 2020 <http://www.ft.lk/front-page/GMOA-s-COVID-19-exit-strategy-advocates-racial-profiling/44-698943> accessed 27 August 2020.

Effective legislative protection of the right to privacy and an awareness of the need for privacy would have ensured that the race/religion of patients infected with COVID-19 remained confidential, without giving room for this information to be used to make unverified and unscientific assertions.

Additionally, concerns such as transparency or accountability remain in the process of contact tracing which was reportedly carried out by intelligence services.[124] In contrast, the approach followed by Singapore is a good example of balancing privacy and public health. The contact tracing mobile application used by the government of Singapore was based on the principle of privacy by design, highlighting the importance of incorporating privacy principles into all aspects of government.[125] A significant shortcoming of the Sri Lankan approach compared to other countries with a more developed approach towards privacy is the lack of emphasis on privacy by all sectors including policymakers, developers of technology, media entities, as well as the general public. Further, considering Sri Lanka's fractured past of ethno-religious violence, targeting of critics and marginalization of minorities, there are also worries that surveillance can be used for extra-legal purposes and requires greater attention.

There are some guidelines that may be of use when exploring this subject. For example, the National Policy on Health Information of 2017 includes policy directives to follow ethical and fair information practices in information management ensuring client privacy and confidentiality.[126] However, there are no specific legal provisions to ensure the confidentiality of medical records.[127] The Code of Ethics for Journalists made by the Press Council of Sri Lanka as well as the Code of Professional Practice of The Editors Guild of Sri Lanka and Free Media Movement

[124] Daily Mirror, 'Intelligence agencies play integral part in tackling COVID-19: Defence Sec.' *Daily Mirror* (Colombo) 18 April 2020 <http://www.dailymirror.lk/breaking_news/Intelligence-agencies-play-integral-part-in-tackling-COVID-19-Defence-Sec/108-186818> accessed 24 August 2020.
[125] Interview conducted by CPA on 06.08.2020.
[126] LIRNEasia, 2018. "*Privacy and Security in Digital Health: Health Data Protection Policy Sri Lanka*". (Digital Health Week 2018).
[127] H Ratnayake, 'Negotiating privacy, confidentiality and security issues pertaining to electronic medical records in Sri Lanka: A comparative legal analysis ' [2013] 4(2) Sri Lanka Journal of Bio-Medical Informatics.

require media professionals to respect the private life of individuals and report personal information only in the public interest as distinguished from public curiosity.[128] Nevertheless, in practice, these regulations are ignored.

The eNIC and National Register of Persons Project

The Department for Registration of Persons (DRP) is vested with the authority to establish a National Register of Persons as an electronic data system and issue Electronic National Identity Cards (eNICs) under the Registration of Persons Act No. 32 of 1968 (as amended).

Laws and regulations governing the eNIC project

1. Registration of Persons Act No. 32 of 1968 as amended by Registration of Persons (Amendment) Act, No. 8 of 2016.
2. Regulations published in Gazette Extraordinary No. 2021/28 of 31 May 2017 made by the Minister of Internal Affairs, Wayamba Development and Cultural Affairs and Gazette Extraordinary No. 2036/9 of 11 September 2017 giving effect to the above regulations.
3. Regulations published in Gazette Extraordinary No. 2115/42 of 21 March 2019 made by the Minister of Digital Infrastructure and Information Technology on the recommendation of the Secretary to the Ministry of the Minister assigned the subject of Registration of Persons.
4. As per Gazette Extraordinary No. 2187/27 of 09 August 2020 the Registration of Persons Act No. 32 of 1968 now comes under the State Minister of Internal Security, Home Affairs and Disaster Management.

The eNIC project seeks to establish a National Register of Persons as a database containing the data of all persons who are citizens of Sri Lanka of 15 years or above, with fingerprints as biometric data and a photograph taken according to ICAO (International Civil Aviation Organization- United Nations Economic and Social Council) standards and issue an eNIC during a specified period of time for the persons completing the eligible age. [129]

[128] Gazette Extraordinary No. 162/5A of 14 October 1981, Rules made by the Sri Lanka Press Council setting out Code of Ethics for Journalists. ; Code of Professional Practice (Code of Ethics) of the Editors Guild of Sri Lanka and Free Media Movement Adopted by the Sri Lanka Press Institute, <https://freemediasrilanka.wordpress.com/code-of-ethics.>

[129] Registration of Persons (Amendment) Act, No. 8 of 2016 [Certified on 07th July, 2016].

On 12 May 2020, issuing a statement via The Presidential Media Division, President Gotabaya Rajapaksa instructed officials to start work on a digital database of citizens.

> *"Individual bio data could be viewed physically as well as through the internet. The new identity card which contains the most accurate data, comprises information required by departments and agencies governed under different laws.*
>
> *It includes information that has to be furnished not only for obtaining passports and driving licences but also for purposes of pension, Samurdhi allowance, income tax and casting vote.*
>
> *The idea of a digital identity card was first mooted by the President when he was the Secretary Defence. The initial preparation relating to the matter commenced in 2012. The new identity card will be prepared by a committee of experts under the direction of Information and Communication Technology Agency (ICTA) and the supervision of a Presidential Task Force."*[130]

Previously, in December 2019, soon after assuming office, the President called for the need to bring all personal information under one data collection centre. The President pointed out that this move will be "instrumental in reducing time, effort and money spent on services such as National Identity Cards, driving licenses, immigration and emigration documents, registration of births and deaths". He also said that by removing the existing practice of gathering the same information by different entities, the government could increase efficiency and prevent the circulation of erroneous and duplicitous information.[131]

---

[130] Economy Next, 'Sri Lanka President instructs to start work on digital database of citizens' *Economy Next* (Colombo) 13 May 2020 <https://economynext.com/sri-lanka-president-instructs-to-start-work-on-digital-database-of-citizens-69903/>

[131] Presidential Secretariat, 'President to explore the possibility of gathering personal information under one data center' (Colombo) 30 December 2019 <https://www.presidentsoffice.gov.lk/index.php/2019/12/30/president-to-explore-the-possibility-of-gathering-personal-information-under-one-data-center/?lang=en>
; Pant M, 'Sri Lankan President calls for a single data collection centre for citizens' personal information' *MediaNama* (India) 6 January 2020 < https://www.medianama.com/2020/01/223-sri-lankan-president-calls-for-a-single-data-collection-centre-for-citizens-personal-information/>

Sri Lanka has both foundational and functional identity systems that are well-developed and robust. Functional identity systems are intended to support a single service such as an electoral or birth registry. A foundational system is where the identifying number is designed to support multiple services, for instance the National Identity Card (NIC) presently obtained from the Department for Registration of Persons.[132] Ownership of the NIC throughout the population is high, reported at 95% for men and 90% for women.[133]

Sri Lanka is in the process of digitizing both functional and foundational identity registries. For example, there have been recent reforms in the digitization of patient records (Patient Health Number-PHN) linked to the national identity, and microchipped drivers' licenses providing details on the holder's ability to operate certain vehicles.

The eNIC has been in development for several years and in October 2017 the DRP started to issue eNICs. These eNICs feature a machine-readable barcode and stored biometric data. So far, the issuance of the eNICs has been limited to those obtaining their NIC for the first time, or those who are renewing their NICs. However, the National Register of Persons has not been set up as yet and successive Ministers in charge of the subject since 2016 have extended the date of expiration of the regulations 'until the necessary infrastructure arrangements and technological methodologies are made to give effect to them'.[134]

Once the National Register of Persons is established, the data in the database would be widely accessible. It could be accessed by any "public officer" or authority in the interests of national security or for the prevention or detection of a crime. The term "public officer" could include most categories of public servants. The term

[132] As per Gazette Extraordinary No. 2187/27 of 09 August 2020 the Registration of Persons Act No. 32 of 1968 now comes under the State Minister of Internal Security, Home Affairs and Disaster Management.

[133] C Handforth, and M Wilson., 2019. *Digital Identity Country Report: Sri Lanka 2019'*. GSMA. Available at: <https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/02/Digital-Identity-Country-Report-Sri-Lanka.pdf > [Accessed 29 July 2020].

[134] Gazette Extraordinary No. 2183/41 of Thursday, July 09, 2020.

"prevention or detection of a crime" is also an extremely broad specification. The mere suspicion of any potential crime, however remote or improbably linked to a person would be enough ground to access the data.

There is no provision for the secure handling of this sensitive data, once legitimately accessed. Even if data is accessed with the best of intentions, carelessness may lead to the information finding its way into the wrong hands. For example, a police officer investigating a suspect may extract the records connected to a person including his family members and then save the data on an unsecured personal computer or leave the printouts on a desk.[135]

In 2017, a Fundamental Rights petition was filed challenging the regulations made to give effect to the National Register of Persons.[136] However, leave to proceed has not been granted in the case as yet. According to information shared with CPA, the Attorney General's Department requested the petitioners to suggest amendments to the regulations which resulted in further delay in the action.[137] The petitioner had suggested that there should be no expiry date on the eNIC card as vast numbers of people could then be denied a vote in a given region or polling division, or many people can be locked out of banking systems or any other government system by delaying their renewal. It was also suggested that as the identity of a person is unique and distinct from that of members of his/her family, there is no necessity to collect information on family members to establish the identity of a person, as the purpose of the DRP was not to maintain an all-encompassing database of all citizens information. Continuing concerns about the lack of an independent civil service, a

[135] Ratnasabapathy R, 'Dangerous data' *Daily News* (Colombo) 18 September 2017 <http://www.dailynews.lk/2017/09/18/features/128484/dangerous-data>

[136] Some of the concerns set out in the petition are as follows;
The nature of the data held in the database would make it a magnet for hackers. The personal data could also be misused by interested parties for personal or political gain, including the targeting of family members of opponents for personal or political gain. The petition further states that the Regulations infringe and/or would imminently infringe the fundamental rights recognized by Article 12 and 14 of the Constitution.

[137] Sunday Times, 'E-NICs: FR petition on alleged invasion of privacy' *Sunday Times* (Colombo) 12 November 2017 <https://www.pressreader.com/sri-lanka/sunday-times-sri-lanka/20171112/281500751534636> accessed 27 July 2020. ; Interview conducted by CPA on 27.07.2020.

history of authoritarian or family rule, and absence of privacy laws was also highlighted. However, CPA was informed that no action has been taken by the Attorney Generals' Department or other authorities to respond to these suggestions.[138]

It appears that under fresh directives by President Rajapaksa the government is working to integrate the foundational eNIC into other forms of functional identity, 'creating interoperability between different identity registers.'[139] However, there is a worrying silence around concern for security measures for these systems. Even as of now, some tender documentation of the eNIC project has been leaked by WikiLeaks, raising concerns about the capacity and the willingness of the authorities to ensure the security of the personal data of a large number of citizens.[140] Legislation on cybersecurity and personal data protection is still at draft stage in Sri Lanka, creating a legal gap.

It will also be necessary for the government to clarify whether the National Register of Persons would be classified as a data controller under the proposed Data Protection Act and whether then, the citizens would have all the rights as data subjects. Additionally, there would be discrepancies between the Registration of Persons (Amendment) Act of 2016 and Regulations made under it and the proposed Data Protection Act. The amendment envisages an invasive model of data collection and processing whereas the draft Data Protection Act is based on the fair information practices and other international standards of data protection.

The introduction of comprehensive and acceptable data protection legislation and ideally, the constitutional protection of the right to privacy must be carried out before the creation of a centralised digital database of citizens' information.

---

[138] Interview conducted by CPA on 27.07.2020.

[139] A. Waidyalankara, 'eNIC in Sri Lanka: Evolution, Revolution, and a looming Breach?' *ReadMe* (Colombo) 23 May 2020 < https://www.readme.lk/enic-sri-lanka/>

[140] Economy Next, 'Wikileaks dumps documents of Sri Lanka's controversial E-NIC project' *Economy Next* (Colombo) 15 April 2019 < https://economynext.com/wikileaks-dumps-documents-of-sri-lankas-controversial-e-nic-project-13686/> accessed 30 July 2020.

Data gathered by surveillance is vulnerable in all the same ways that other data are vulnerable: vulnerable to misuse, to misappropriation, to hacking, to loss, to corruption and error. Linking multiple data sets to form a single central database creates a "single point of failure." More linkages also increase the risk of identity theft as "the more places people use it, the risk of identity theft increases."[141] Additionally, an all-encompassing compulsory digital identity system has the potential to turn into a mass surveillance system of the populace by the State. Past experience has demonstrated that far less sophisticated systems have been used by the State to surveil and intimidate journalists, activists, political opponents and others critical of government policy.

Additionally, such a centralized digital database performing the functions of both foundational and functional identity creates a new power centre wherein a single body has the power to delist an individual from the database, thereby potentially denying them essential services, welfare and other rights of a citizen. The present legislation and regulations do not provide for the transparency and accountability of the decision-making authority and power is concentrated in the Commissioner-General. Section (9) (2) of the regulations provides this power to the Commissioner-General to block an ID under an "exigent condition".

CPA notes that in the event the system fails, people will likely be deprived of fundamental freedoms. A variety of reasons such as power failure, connection failures and system failure, missing fingers and other forms of disability, as well as the expiry of cards could exclude persons who would then become a non-person. Additionally, a central database with data of all citizens would be a magnet for hackers and those trying to make money from personal data.[142]

---

[141] B. Solomon, Digital IDs Are More Dangerous than You Think' *WIRED* (New York) 20 September 2018 < https://www.wired.com/story/digital-ids-are-more-dangerous-than-you-think/> accessed 30 July 2020.

[142] R Ratnasabapathy, 'Sri Lanka's plans to move to a digital ID promises benefits but carries grave risks' (*Echelon*, 3 October 2017) <https://www.echelon.lk/sri-lankas-plans-to-move-to-a-digital-id-promises-benefits-but-carries-grave-risks/> accessed 24 June 2020.

As per Gazette Extraordinary No. 2187/27 of 09 August 2020 the Registration of Persons Act No. 32 of 1968 now comes under the State Minister of Internal Security, Home Affairs and Disaster Management. A Cabinet Minister for the subject of Defence has not been assigned (with only the State Minister of Defence appointed). The Secretary to the Ministry of Defence is Major General (Retd) Kamal Gunaratne. The non-appointment of a Minister of Defence creates a responsibility and accountability gap.

Additionally, retired military personnel being in charge of the registration of persons raises concerns about the militarization of civil functions within Sri Lanka's public administration and development sectors.[143]

It is maintained that a database such as the National Register of Persons would allow the large number of Sri Lankan migrant workers to meaningfully exercise their right to vote in elections. During the 2015 constitutional reform project, the PRC discussed this possibility in detail and while supportive of the idea of the right of migrant workers to vote felt that it was necessary to be cautious when using an electronic voting system as it could lead to invasions of privacy and the surveillance by the State of individuals.[144]

The eNIC and National Register of Persons project also came under scrutiny in Parliament in 2014. Opposition MPs claimed that the right to privacy of citizens will be violated by introducing a program to collect personal details of the individuals as well as their families to establish a national data base.[145] Objections were also raised to including biometric identification details, stating that at present, only criminals are fingerprinted, but under this new system, every citizen will be fingerprinted and

[143] From 2011 the Registration of Persons Act was under the Ministry of Defence. After 2015 thus was transferred to the Ministry of Internal Affairs and then the Ministry of Digital Infrastructure. It is now again under the Ministry of Defence.

[144] Public Representations Committee on Constitutional Reform, 'Report on Public Representations on Constitutional Reform', 2016.

[145] Kirinde, C., 'Concerns, misgivings, unease aside, e-NIC set to invade individual privacy' *The Sunday Times* (Colombo) 31 August 2014 < http://www.sundaytimes.lk/140831/news/concerns-misgivings-unease-aside-e-nic-set-to-invade-individual-privacy-115956.html>

all their personal data will be stored and accessed by the authorities at any time.[146] The use of biometric data is problematic under the best of circumstances due to inherent weaknesses in terms of security and access. The use of biometric identification needs the developments of special legal procedures and evidentiary standards to protect human rights and due process.

MPs from the opposition further stated that while they were not opposed to the eNIC being issued, seeking people's personal details in violation of all international covenants, would not be necessary for this. The importance of transparency, accountability and participation of all stakeholders in the process was emphasized. In 2014, at the time this project was first proposed, the Registration of Persons Department was under the Ministry of Defence. Parliamentarians also argued that it should be brought under the Ministry of Internal Affairs, as this was a task to be done by civil institutions, protecting people's privacy. As at present, the Registration of Persons Department is under the State Ministry of Internal Security, Home Affairs and Disaster Management.[147] This concern is even more relevant now in the context of increasing militarization of civilian institutions.

MPs from the Tamil National Alliance (TNA) raised further concerns regarding the issuing of an eNIC, saying it could lead to racial profiling and be used against the Tamil population.[148] It was stated that the information collected could be used to monitor people. This would also increase concerns surrounding the large-scale land grabbing in the North, where this kind of data can be used to further these land grabs.[149]

The emphasis on the proposed benefits of the National Register of Persons flows from the portrayal of data as the ultimate solution to everything. When data is put forward as a resource to be mined, it is believed to somehow yield ultimate truth. In

[146] ibid.

[147] As per Gazette Extraordinary No. 2187/27 of 09 August 2020.

[148] Kirinde, C., 'Concerns, misgivings, unease aside, e-NIC set to invade individual privacy' *The Sunday Times* (Colombo) 31 August 2014 < http://www.sundaytimes.lk/140831/news/concerns-misgivings-unease-aside-e-nic-set-to-invade-individual-privacy-115956.html>

[149] ibid.

other words, data has effectively emerged as the twenty first century's oracle. This leads to the race to find simplistic technological solutions to complex social problems. This representation of the infallibility of data is based on the assumption that information yielded by the datafication of lives is more objective and accurate than anything that has come before, which is an assumption that must be questioned and critically evaluated. [150]

Case studies from comparative jurisdictions

Case study 1 – United Kingdom

Identity Cards were first used in the UK during the two World Wars—first under the National Registration Act 1915 and then under the National Registration Act 1939. Following a court ruling that called into question the legality of continuing to use a power given during a national emergency when the emergency no longer existed, wartime identity cards were formally ended in May 1952.

The Identity Cards Act 2006 created a framework for national identity cards and a national identity register (NIR) in the UK.

However, following concerns with regard to personal liberty and arbitrary use of state power, the Identity Documents Act 2010 was passed. The Act cancelled ID cards and enabled the disposal of information recorded in the NIR. The UK national identity card ceased to be a legal document for confirming a person's identity and all data was "securely destroyed" along with the NIR in February 2011. Around 500 hard disk drives and 100 back-up tapes containing the details of 15,000 holders who were part of the pilot project were magnetically wiped, shredded and incinerated in line with Cabinet Office rules.

[150] A Kovacs, 'When our bodies become data, where does that leave us?' (*Internet Democracy Project*, 15 June 2020) <https://internetdemocracy.in/reports/when-our-bodies-become-data/> accessed 4 August 2020. ; Tucker, I., 'Evgeny Morozov: 'We are abandoning all the checks and balances'' *The Guardian* (London) 9 March 2013 <http://www.sundaytimes.lk/140831/news/concerns-misgivings-unease-aside-e-nic-set-to-invade-individual-privacy-115956.html>

Home Office minister Damian Green said: 'Laying ID cards to rest demonstrates the government's commitment to scale back the power of the state and restore civil liberties.'

It must be noted that many democratic nations— UK, USA, Japan and Australia — as yet, function perfectly well without ID cards of any form.

Case study 2 – Uganda

A study on Uganda's Digital ID System found that only 12% of respondents had received their National IDs at the time although a proportion of 88% had submitted their registration forms, depriving over 80% of essential services such as SIM card registration. The enjoyment of fundamental freedoms and rights is arbitrarily curtailed due to this.

In 2017, citizens' personal data collected by National Identification Regulatory Authority of Uganda for the project was breached while in the possession of third party private entities. This data was used for criminal activities including the fraudulent extortion of Shs 51m (equivalent to USD 14,206) from Roko Construction Company. This was despite the right to privacy being a fundamental right under the 1995 Constitution of Uganda.

The Ugandan Police is taking steps to integrate its CCTV system with the National Identification Regulatory Authority of Uganda to create a National Command and Control Centre 'to make the presence of the Police felt within the community.'

Case study 3 – India

The experience in India shows that a National Digital Identity system in the absence of data protection laws and citizens' right to legal recourse could have disastrous consequences. The Aadhaar system initiated without a data protection law resulted in the Aadhaar Database Hack in 2018 where the biometrics and personal information of over 1 billion Indians were compromised.

The authentication mechanism under Aadhaar system leads to the creation of authentication logs. Each time Aadhaar is used to authenticate one's identity, the

log notes metadata of such authentication. Experts have noted that when done at scale and over a long period of time, such authentication logs can be a tool for pervasive profiling and surveillance.

Apart from this, countless instances of exclusion of citizens from benefits due to failures within the system are reported. This has especially been for those who need these benefits most, such as rural populations, daily wage earners and those with disabilities.

Case study 4 – Pakistan 'a privacy nightmare'

In 2001, the National Database Registration Authority (NADRA) was created to computerize all citizen data. In 2007, NADRA introduced a multi-biometric system. By now, NADRA has issued 91 million computer generated cards, which is 96% of the entire adult population. It is one of the world's largest national databases.

Rampant identity theft compelled the state to do a wholesale re-registration of IDs in 2016. But as of 2019, a website with no apparent details of ownership is providing citizen details including current and permanent addresses, date of birth, mobile phone numbers and more, with an accuracy rate of above 90%.

Additionally, thousands of citizens in Pakistan have had their CNIC's "blocked" on suspicion of being aliens, making them stateless. They are unable to purchase a mobile phone connection, obtain connections for utilities, sell or purchase land, travel or deal with a bank.

Section (9) (2) of the regulations in Sri Lanka provides similar powers to the commissioner general to block an ID under an "exigent condition".

The system has also enabled mass surveillance in Pakistan.

1. Geo-fencing

The Pakistani police use GPS or RFID technology to create a virtual geographic boundary, enabling software to trigger a response when a mobile device enters or leaves a particular area. The police get the mobile numbers of people, now readily accessible on the database.

2. Hotel Eye

This system logs the check-ins and checkouts of guests at hotels, along with CNIC numbers and personal details.

The eNIC system of Sri Lanka is modelled on Pakistan's CNIC system.

V. Conclusion

The protection of the right to privacy is dependent on dispelling the image of privacy as a concept that is anti-progressive, overly costly, and hostile to the protection of social interests. To counter this narrative, it is necessary to articulate a comparably convincing description of privacy's importance to all individuals and 'the political and intellectual culture' that we value, as privacy exists beyond legal and technological frameworks and is directly related to human and social concerns.

There is no express protection of privacy in the Constitution or other legislation in Sri Lanka. Personal information is shared incautiously and personal data is harvested routinely for marketing and misused. This has been worsened by decades of conflict and ethnic violence, and rule under emergency powers. Privacy is perceived as being dispensable for the protection of common interests, when in fact a balance between individual and collective interests would serve to more effectively protect common interests. This paper suggests that while the constitutional protection of the right to privacy is essential, this alone would not ensure the protection of the right in practice. Legislation, access to legal remedies, an effective institutional framework as well as cultural transformation is indispensable to counter the culture of eroding privacy for expediency which could potentially undermine the right to privacy further.