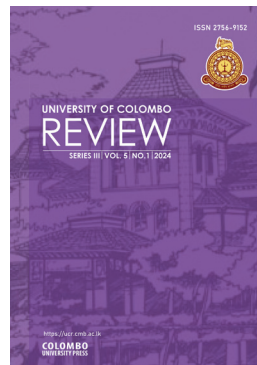


DOI: <https://doi.org/10.4038/ucr.v5i1.158>

University of Colombo Review (Series III),
Vol.5, No.21, 2024



An analysis of privacy policies in Sri Lanka

Tavini Nanayakkara

Lecturer, Department of Private and Comparative Law, University of Colombo, Sri Lanka

ABSTRACT

This article focuses on privacy policies of websites and attempts to understand how they have been designed. A study looking at the privacy policies of US firms was conducted for the first time in 2016 by Professor Marotta-Wurgler. While the study provides a look into how the global north considers privacy, there is nascent scholarship in this regard for the global south. I look to the global south – Sri Lanka, in particular – to understand to what extent privacy and the well-being of consumers feature in designing privacy policies of various industries in the country. I look at 20 privacy policies across four industries, cloud computing, banking, supermarkets, and transport services. I conclude that while firms abide by some international standards even without legal obligation, there is room for improvement. There is little standardization within and across industries with international firms laying down higher privacy protections on average. The article finds most policies to be long and incomprehensible. I conclude that while incorporation of international privacy standards to varying degrees absent legal compulsion is admirable, there is more to be done to benefit the consumers for whose welfare privacy policies are drafted in the first place.


KEYWORDS:

Privacy policies, General Data Protection Regulation, Personal Data Protection Act, Sri Lanka, Cloud computing, Banking, Supermarkets, Transport

Suggested Citation: Nanayakkara, T (2024). An analysis of privacy policies in Sri Lanka. University of Colombo Review (New Series III), 5(1), 79- 103

© 2024 The Author. This work is licenced under a Creative Commons Attribution 4.0 International Licence which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

✉ Corresponding author: tavini@law.cmb.ac.lk

 <https://orcid.org/0009-0007-8350-3728>

Introduction

In today's digital markets, online privacy policies are inescapable (Jensen & Potts, 2004). While there is little doubt about the widespread existence of privacy policies, many details about how privacy policies are drafted, their content, and friendliness towards consumers, especially in Sri Lanka remain unanswered, although studies have been conducted in other jurisdictions. Many questions abound, including how are these privacy policies designed? To what extent are international privacy standards incorporated in the print? Are the terms used to set out the levels of data privacy that will be adopted by different firms and industries the same? Are the contracts meant to be long winding so that consumers cannot keep up? Do companies try to make the contracts more understandable for their customers? These are all questions worth our time, *albeit* left largely unattended in scholarship in developing countries, barring a few exceptions which are discussed in greater length in the literature review section below (Chatsuwan et al., 2023; Jayed et al., 2020; Bareh, 2021; Maraba et al., 2023).

This article is modelled after Prof. Marotta-Wurgler's 2016 pioneering study (Marotta-Wurgler, 2016), where she analyzed a sample of 249 privacy policies in a range of different industries in the US in order to determine how companies go about designing their contracts. She concluded that privacy policies' content is shaped by market forces as much as by self-regulatory regimes based on external guidelines (Marotta-Wurgler, 2016). Other studies conducted on privacy policies on a global scale, on the United States, and Asia have shown disappointing practices and standards with regard to data privacy, with some improvement in privacy policies in Europe post-enactment of the GDPR.

This article focuses on the global south and Sri Lanka, in particular, where I look at privacy policies in four different markets in order to analyze six main questions: (i) to what extent do the privacy policies of firms operating in Sri Lanka incorporate international privacy standards? (ii) is there standardization of terms relating to data privacy within each industry? (iii) is there standardization of privacy terms across industries? (iv) is there a difference in the privacy terms of local and international firms? (v) what is the length of privacy policies? and (vi) what is the level of readability of privacy policies? In looking for answers to these questions, I look at 20 privacy policies, across the industries of, (a) cloud computing, (b) banking, (c) supermarket, and (h) transport services. I chose these industries due to their high use by consumers in Sri Lanka which would be rich ground to analyze their concerns of data privacy while receiving these services. The respective firms within each industry were randomly selected and in a greater majority of cases were the only firms that operated in Sri Lanka or had adopted privacy policies. The number of privacy policies that were considered from each industry are set out below along with whether they are international or domestic firms (Table 1).

Table 1: Breakdown of number of privacy policies considered along with their status of international or domestic firms

	Cloud Computing	Banking	Supermarket	Transport services
Number of privacy policies considered	5	5	6	4
Number of privacy policies of domestic firms considered	1	3	4	3
Number of privacy policies of international firms considered	4	2	2	1

The article proceeds on the hypothesis that enterprises that operate in Sri Lanka adopt privacy policies that are standardized within and across industries and given the low priority by Sri Lankan firms to privacy, considerably diverges from international privacy standards.

For the sake of completeness, first, I lay down the domestic law pertaining to privacy and compare it with international standards, the General Data Protection Regulation ('GDPR') (GDPR, 2016) in particular. Next, I review the literature on the area. Afterwards, I present the empirical findings from the four markets. Following this, I engage in an analysis of the patterns that emerge across and within the various industries. The article concludes that, the privacy policies of firms that operate in Sri Lanka are designed with some attention to international standards even without any legal obligation. The study found that there is little standardization within and across industries. International firms, on average, promise greater protections than local firms. On the whole, however, all contracts can be more consumer-friendly in terms of length and readability. It recommends firms, regardless of the industry, align with international standards, not only for the sake of global compliance but also for the sake of consumers who are most affected by weak privacy protections.

This article is part of a broader study that is meant to be conducted over several years in analyzing the implementation of privacy legislation in Sri Lanka. This is the first instalment that considers the status of privacy policies before the Personal Data Protection Act 2022 (Sri Lanka) has completely come into effect. Future study will look at whether the status quo changes with the Act coming into effect and Sri Lankan firms presumably developing greater familiarity with its obligations on personal data protection.

This study is limited to a comparison of privacy policies that have been drafted and does not venture into whether firms comply with the statements of privacy which would be most telling in exploring the privacy culture of Sri Lanka. The sample sizes remain small, compared to other studies done in foreign jurisdictions, especially in

the global north. Although this is mainly due to the smaller market in Sri Lanka, the small sample size can be problematic in drawing statistical conclusions. Nonetheless, as a first of its kind study done on privacy policies in Sri Lanka it would be useful in identifying the practice of firms in different industries in order to identify the culture of data privacy in the country prior to coming into effect of binding legislation. Lastly, this study is limited to the extent of examining privacy policies in the English language in Sri Lanka.

Law regarding privacy in Sri Lanka

Domestic law governing privacy

The Constitution of Sri Lanka does not recognize a fundamental right to privacy. While the residuary law in the country which is the Roman-Dutch law recognizes privacy under the *actio injuriarum*, this action has not been used to safeguard data privacy. In fact, multiple South African commentators who have written on the action have recommended that separate personal data privacy legislation be enacted to ensure protection of consumer rights (Neethling *et al.*, 2005). Nor does international law contain binding obligations of data privacy that Sri Lanka has taken on.

However, in 2022, Sri Lanka took company among several other nations in South Asia that were in the process of putting into place data privacy legislation, voluntarily taking on a heightened level of privacy related to personal data.¹ It surpassed the rest of the South Asian nations early last year when it enacted one of the first comprehensive laws in personal data protection among the countries in South Asia – the Personal Data Protection Act No. 9 of 2022 ('PDPA') on the 19th of March 2022.

However, before all the provisions of the Act come into play, controllers and processors have been given a grace period of 18 to 36 months to become PDPA-compliant (*Personal Data Protection Act (PDPA), 2022*, section 1(3)). Therefore, this study would be telling of how industries model their privacy policies when there is no direct and mandatory legal obligation to abide by.

Comparison with international standards

The GDPR is considered the gold standard in data protection (Taylor, 2020; Mantelero, 2020). I use this as a benchmark to compare the PDPA with for two reasons. First, it is considered to be the highest standard of personal data protection due to the safeguards it provides to consumers' data (Taylor, 2020; Mantelero, 2020). Second, the drafters of the PDPA itself have spoken of how they took into cognizance

¹ Some other states that were contemplating adopting privacy legislation are Bangladesh, Pakistan and India.

obligations under the GDPR when drafting the PDPA (Fernando & Wickramasinghe, 2022). Due to the PDPA's purpose of ensuring cohesion with international standards in order to enable cross-border data processing, it contains, to the greatest extent, the obligations in the GDPR, with certain changes appropriate for a developing country such as Sri Lanka. I engage in this comparison in the portions that follow.

Both the GDPR and the PDPA encompass similar principles relating to lawfulness (PDPA, section 5; GDPR, articles 5(1)(a) and (6)), purpose specification (PDPA, section 6; GDPR, articles 5(1)(b)), purpose confinement (PDPA, section 7; GDPR, article 5(1)(b)), data retention (PDPA, section 9; GDPR, articles 5(1)(e)), accuracy (PDPA, section 8; GDPR, articles 5(1)(d)) and integrity and confidentiality (PDPA, section 10; GDPR, articles 5(1)(f)). One of the differences between the PDPA and the GDPR is how the former treats the principles of transparency as a stand-alone principle of processing while the GDPR recognizes transparency in connection with data subjects' rights (Fernando & Wickramasinghe, 2022). Accountability has been set out with a number of obligations including data protection management programs and compliance mechanisms.

The PDPA also places emphasis on data subjects' rights such as right of access (PDPA, section 13; GDPR, Article 15), withdrawal of consent (PDPA, section 14; GDPR, Article 7), rectification (PDPA, section 15; GDPR, Article 16) and erasure (PDPA, section 16; GDPR, Article 17). One difference, however, is the exclusion of data portability (GDPR, Article 20). In a publication by two of the drafters of the legislation it is stated that this was decidedly left out *"due to the lack of maturity in Sri Lanka to effectively implement such technically specific statutory obligations"* (Fernando & Wickramasinghe, 2022).

Furthermore, the PDPA and the GDPR include the right to object. Section 14 of the PDPA stipulates the right to withdraw consent along with the right to object while section 14(2) proceeds to stipulate this right with regard to personal data and sensitive data processed further to the public interest or legitimate interest of the controller or third party overriding the interest of the data subject. The GDPR in article 21 stipulates a similar right with special reference to data processed for marketing purposes. Therefore, on the whole, the two rights are laid down in broadly similar terms.

An important nuance can be seen with regard to automated decision-making in the PDPA and GDPR. The PDPA in section 18 mentions that every data subject has the right to request a controller to review a decision that is solely made through automated means and is likely to create an *"irreversible and continuous impact on the rights and freedoms of the data subject..."* However, this is subject to several exceptions such as automated data processing being authorized by written law, by the authority, consent of the data subject and is necessary to enter into the contract. The GDPR also mentions automated decision-making under article 22 which provides the

right to data subjects not to be subject to decisions made solely by automated means “...which produces legal effects concerning him or her or similarly significantly affects him or her.” Similar to the PDPA this too is subject to exceptions such as situations where such automated decision-making is necessary for entering into the contract between the data subject and data controller, authorized by law and based on the data subject’s consent. The main difference appears to lie in phrasing used to shield data subjects from automated decision-making. While the PDPA refers to “irreversible and continuous impacts on the rights and freedoms of the data subject” the GDPR refers to “legal effects” or effects that “significantly affect him or her”. In a sense, the GDPR through a literal interpretation appears to encompass more situations in which data subjects may be exempted from automated decision-making.

Therefore, on the whole, the PDPA stands on par with the best of the legislation regarding consumer privacy. Nevertheless, this legislation remains unenforceable until after the grace period of 18 to 36 months – the time to be specified by the relevant minister (PDPA, section 1(3)). The date of operation for the provisions of parts VI, VIII, IX and X of the PDPA has been set at the 1st of December, 2023, while the date of operation for the provisions of parts I, II, III and VII have been set as 18th March 2025. Given that the principles being considered in the current article are contained in parts II and III, which are yet to be brought into operation, firms in Sri Lanka remain unbound by the obligations. Therefore, this article looks at whether firms in Sri Lanka abide by recognized principles of data privacy absent legal compulsion.

Previous studies on privacy policies

This section sets out some empirical research that has been conducted thus far on privacy policies around the world. While many studies have been carried out on particular sectors, and for the most popular websites in the world or the global north, a handful of scholars have focused on some global south countries as well. The findings are interesting in how they allow to situate the current article. This is through depicting the absence of previous study conducted in Sri Lanka and how the findings help confirm some generalized findings that have been made for South Asia previously.

Some empirical work had been conducted on privacy policies prior to the enactment of the GDPR where the standards were measured with regard to fair information practices around the world. One study which considered a hundred websites’ privacy policies around the world from the financial, news, adult, social, blogging, search engines, job, games, healthcare and dating industries saw how user information was vulnerable to being passed on to affiliates and third parties after being collected by various firms (Brown *et al.*, 2012). This study also looked at the readability of privacy policies of different firms, where healthcare and dating sites

were found to be specifically hard to read. A study published in 2019, using the experience of 749 internet users with privacy policies demonstrated that they found policies difficult to understand, across the board (McDonald *et al.*, 2009).

While there is some merit to the argument to the effect that these deficiencies dramatically changed after the enactment of the GDPR, the argument applied only to select countries and sectors. For instance, in United States of America (US), which does not have national legislation akin to the GDPR, a study looking at 600 companies with regard to 10 privacy pertinent factors found that there was a considerable percentage of sites even by 2017 that lacked privacy policies altogether (Zaeem *et al.*, 2017). The study also showed that the rest of the sites collected information of users claiming to only utilize them for specific purposes on paper but in practice revealed information to law enforcement authorities without following due procedure. Further, it was found that these sites post new privacy policies with no notice which would require customers to frequently check said policies. Another study of 23 airlines in the US found that air travel was significantly lagging behind in its fair information practices (Nyshadham *et al.*, 2000). A study published recently on privacy policies of the US focuses on the effectiveness of self-regulation in industries compared to government regulation and comes to the finding that in certain sectors, such as the industry sector which is self-regulated, there is greater adherence to professed privacy practices and fair information practices as opposed to the highly regulated financial sector (Jiang *et al.*, 2023). Overall, the study finds that there is more to be done in enforcement of privacy policies in the United States, in general.

Apart from these, it was interesting to come across a study that was also done to compare the effect of the GDPR pre and post its enactment on a total of 1000 privacy policies around the world (Zaeem *et al.*, 2020). It concluded that there was progress in how users' data is being handled and that the most significant increase has been the allowances made for users to edit and delete information and to share information with law enforcement. If privacy policies fell short, it was in their lack of showing levels of compliance which translated to a lack of transparency and disclosure regarding how personal information of its customers were being handled (Zaeem *et al.*, 2020). A similar study was conducted on 500 sites in Europe which showed that, there was improvement in the privacy policies, where, a great majority had updated their policies, while some had newly created privacy policies and others went onto display cookie consent notices (Degeling *et al.*, 2018). The study went further and identified changes that need to be made when it comes to implementation, especially with regard to third party cookies.

There have been a handful of studies done on the global south as well. In one study, the authors developed a quantitative method for evaluating compliance with privacy policies through a scoring model that is connected with methods of statistical

data analysis and went on to apply this tool to Small and Medium Enterprises in Thailand (Chatsuwan *et al.*, 2023). The results showed significantly low scores and the article moved on to provide suggestions on how levels of compliance may be increased. A study done on a total of 284 websites in India, Pakistan, and Bangladesh with regard to the sectors of e-commerce, finance, education, healthcare, news, government, telecom, buy and sell, jobs/freelance and blog/forum showed similar disappointing results (Jayed *et al.*, 2020). There was low accessibility in education, healthcare and government sectors and low readability for privacy policies of all three countries. The highest compliance was shown for processing of data and third-party transfers. The article concluded with suggestions on how stakeholders can improve data privacy in South Asia. India was included in another study (Bareh, 2021) which analyzed 130 academic websites of India's Institutions of National Importance. The study revealed, across the board, security vulnerabilities, low readability, lack of cookie consent as well as web-tracking. Finally, a study done on the privacy policies of 18 retail websites in South Africa analyzed if they met the standards set by relevant national guidelines and the requirements of the Protection of Personal Information Act and found that while all 18 websites had a privacy policy, some fell short of the required standards (Maraba *et al.*, 2023).

As the discussion on previous studies on privacy policies reveals, comparatively, more work has been done in the global north and worldwide as opposed to the global south. Within the global south, there is limited attention paid to South Asia, aside from the usual suspects of India, Bangladesh, and Pakistan.

The current study, with its particular focus on Sri Lanka, looking at privacy policies across several industries stands apart. One respect in which it is novel is that it focuses on Sri Lanka, hitherto unnoticed, but second, it not only looks at the policies in terms of compliance with international standards but standardization within and across the industries as well. It makes an effort to understand the privacy culture that currently exists without a legal landscape regarding personal data fully coming into effect. With the Personal Data Protection Act coming into effect in full by 2025, it would be interesting to compare current findings and assess if there is actual enforcement of and compliance with local data privacy laws, after the entire Act comes into operation.

Empirical findings

This section presents quantitative and qualitative findings that emerge with regard to the (i) level of acknowledgement of international standards in the privacy policies, (ii) level of standardization of different privacy terms within industries, (iii) level of standardization of privacy terms across industries, (iv) comparison between privacy policies of domestic and international firms, (v) length and (vi) readability of privacy contracts. The work that is reflected in the current section was carried out during 2023.

To begin with, it is interesting to note that certain firms do not appear to have privacy policies in the public domain that could be readily accessed. Oddly enough, this was the case for one recognized local private sector bank and less shockingly so for two firms in the transport services sector. All firms in cloud computing and supermarkets, however, had readily available and accessible privacy policies. The firms which did not have privacy policies were not factored in the samples and when calculating average figures for industries.

Level of acknowledgement of GDPR standards in local and international firms

It is heartening to note that there appears to be much higher attention paid to GDPR standards on a voluntary basis by firms and industries across the board. Whether the firms actually put into practice the heightened obligations they voluntarily take on is not a question that can be answered here as it would require observation of these firms in practice, the availability of certain privacy terms, however, provides evidence of importance being paid to acknowledge international standards (See table 2).²

Table 2: Acknowledgement of international standards by firms

This table has chosen a few of the most salient international privacy principles contained in the GDPR, most of which are also encompassed in the PDPA in order to assess acknowledgement of international standards by companies

		Full sample N = 20	Cloud computing N = 5	Banking N = 5	Supermarket N = 6	Transport N = 4
1.	Legal basis	95%	100%	100%	100%	75%
2.	Disclosure of purpose	95%	100%	100%	100%	75%
3.	Disclosure of processing personal data and the types of data so processed	95%	100%	100%	100%	75%
4.	Period of retention	65%	80%	80%	50%	50%
5.	Data subjects' rights					
	• Access	80%	80%	80%	83.33%	50%
	• Rectification	75%	80%	80%	83.33%	50%
	• Restriction	50%	80%	40%	33.33%	50%
	• Deletion/erasure	50%	80%	40%	33.33%	50%
	• Portability	30%	40%	40%	16.67%	25%
6.	Security	70%	80%	100%	83.33%	0%
7.	Disclosure/sharing of data	90%	100%	80%	100%	75%

² See section entitled 'Comparison with international standards' for relevant international standards.

The highest levels of incorporation of international standards can be seen in cloud computing with the banking sector following closely behind. All the firms in the cloud computing industry alluded to the relevant laws of specific states which would determine how the policies would be implemented in the respective jurisdictions. Only the cloud computing service in Sri Lanka makes explicit reference to the Personal Data Protection Act of Sri Lanka. No other local privacy policy in any industry that is included in this study makes such explicit reference.

Most of the industries did not appear to specifically refer to the legal basis on which the personal data of consumers was collected apart from one international firm in cloud computing (Company B). Almost all firms across the board alluded to either consent of the data subject or necessity in order to provide the relevant service as the legal bases for collecting, processing, storing and using personal data of its consumers. All firms in all areas, to different degrees laid out the kinds of personal data and the purposes for which the data was collected. While these were not exhaustive lists, they provided adequate detail in order to notify consumers.

While almost all firms in the cloud computing and banking sectors referred to how long they plan to retain the personal information of their consumers, the supermarket and transport industries paid less attention to laying out this detail.

Varying levels of attention were afforded to rights of data subjects such as right of access, rectification, restriction, deletion, and portability. The cloud computing industry appears to pay the most attention to these rights. The banking and supermarket sectors have an average and similar level of consideration of said rights. The right to portability of data appears to be paid the least attention to across all industries. The right to restrict and erase one's personal data was at a higher level with the right to access data being the right that is most widely acknowledged with the right to amend and rectify a close second. Only half of the firms in the transport industry seem to consider the rights of data subjects at all.

The most unexpected finding is the absolute disregard of the transport sector in notifying the consumer as to how they plan to safeguard the personal data they collect. All other industries pay the highest attention to this element with only one firm in cloud computing and the supermarket industry failing to mention it. Almost all the sectors claim to refrain from selling their consumers' data and are only shared with consent or when necessary, according to the law.

Therefore, if one were to rank incorporation of international standards and now even national standards in Sri Lanka, cloud computing is found to be the most compliant. This is followed respectively by banking, supermarket, and transport industries.

Standardization within industries

While there is similarity in the provisions that are available within each industry as can be seen above, the level of detail and care taken in stipulating different provisions is stark in almost every industry. ‘Standardization’ is used in this study to denote the similarity of privacy policies in comparison to each other.

Cloud computing

As a precursor, the privacy policies that were looked at for cloud computing do not specifically refer to the cloud computing service only but for the range of services provided by the company, of which cloud computing is but one. Only one firm contained a separate privacy policy for the cloud. However, this was considered along with its general policy as it contained far more information which should be considered in understanding the level of concern the firm pays to the privacy of its customers, including those that utilize its cloud computing services.

While all the firms look to have the same provisions present, their content looks anything but standardized. Although there are similarities, the structure, the level of detail and the manner of explanation differ. For instance, when it comes to the kinds of information that is collected, all five firms provide non-exhaustive lists while some firms go the extra step of mentioning information the firm collects, information that is automatically stored and the information that is collected from other sources. The purposes for which the data is used appear to be similar ranging from provision of the relevant service, to communicate with the consumer and to improve the service and ensure protection of the data.

Across the board, data appears to be retained “as long as necessary” to provide the service and to comply with legal requirements. However, it is interesting to note that these firms do not mention how they would determine the period of retention that is necessary in the absence of an explicit reference to a date or time period.

When sharing data, the firms all contend in different ways to do so with consent or to abide by legal requirements and to carry out business transactions. Interestingly, however, one international firm takes on the obligation to defend its customers’ data from governments. It goes to the extent of stating,

“...We believe that all government requests for your data should be directed to you. We do not give any government direct or unfettered access to customer data. [Company E] is principled and transparent about how we respond to requests for data. Because we believe that you have control over your own data, we will not disclose data to a government except as you direct or where required by law. [Company E] scrutinizes all government demands to ensure they are legally valid and appropriate.”

However, this appears to be an outlier in duties taken on by cloud computing services.

The security aspect differs although most of the firms, especially the international firms, seem to make the provision of secure services a primary concern through different means including various physical, electronic, and procedural safeguards. An outlier is the domestic firm that was considered in the sample (Company A) which appears to explicitly reduce its responsibilities by disclaiming that,

“...The security of your data is important to us but remember that no method of transmission over the Internet or method of electronic storage is 100% secure. While we strive to use commercially acceptable means to protect your Personal Data, we cannot guarantee its absolute security.”

Lastly, when it comes to the rights of data subjects, each privacy policy lays out how the consumers may exercise their rights. In fact, certain policies provide further links to additional information on how these rights may be enjoyed. Not to mention, they refer to certain jurisdictions with special privacy standards according to which they claim to implement the privacy policies.

Banking sector

In the banking sector, there is a divergence between the quantitative findings mentioned in the section entitled ‘Level of acknowledgement of GDPR standards in local and international firms’ and the qualitative findings in this section. To begin with, however, a similarity – the guarantee of security of personal data of customers that is collected by banks appear to show similarity in their level of cognizance of the sensitive nature of the information they handle and the requirement to implement adequate measures to ensure its safety. The policies also warn consumers to refrain from making themselves vulnerable to online fraud and theft and cautions customers to refrain from sharing sensitive information through unprotected forums. A divergence, however, is the manner in which the rights of data subjects are laid out. While quantitatively it appeared to be at a high level, the level of detail given to enunciating the rights differs across different banks. This difference can be found in the terms dealing with the sharing of data as well, where majority sets out the parties with which the data will be shared, Company P’s policy omitted to mention it at all, while another simply said “shared only for law enforcement purposes”. Firms in the industry tended to give specific figures regarding the period of retention such as five and seven years, while others went with the signature clause of “no longer than necessary”. The kinds of information that is collected and the purposes of collection appeared to be similar enough although no carbon copies of each other.

Supermarket industry

The kind of personal information collected and the purposes for which the information would be used appears to be similar within the supermarket industry. The firms seem to want to retain information as long as is necessary with one firm

alluding to a minimum of 7 years. Almost all privacy policies state that they do not sell the data of their customers and lay out lists of parties that the information is shared with. On the whole, there is not much deviation in the content. However, the wording that is used and the manner in which the information is presented are different for each firm.

Unlike banking, and more like the cloud computing industry, there is greater mention of the rights of data subjects in different jurisdictions. Two privacy policies, one foreign and the other local refer to rights of data subjects in other jurisdictions specifically the EU (Company J and G), while the foreign firms refer to data subjects in other jurisdictions such as the state of California in the USA (Company J) and Dutch law (Company I) where it states, “... you agree to submit to the courts of Amsterdam, Netherlands over any claim or matter arising under or in connection with these terms.”

Transport industry

The transport industry appears to be the most elusive in terms of ready accessibility of privacy policies. Two of the firms that were to be included in the sample originally had no privacy policies that were available online. Two of the other firms that were included in the sample had little to no detail on how personal information of consumers was to be collected and used (Company N and O). This leaves two firms – one international and one domestic (Company L and M).

In comparing the two, we find that the terms of the international firm refer specifically to certain jurisdictions in which users would have different privacy rights and controllers and processors of personal information would have different obligations. However, the domestic firm also makes allusion to the fact that data might be transferred to other countries which may have comparatively less protective laws but that reasonable measures will be taken to protect personal information as well the rights to access, correct and delete data in line with applicable law.

The two firms in the transport industry with comprehensive data protection provisions do not constitute the most fertile ground for a comparison. However, it provides insight into how international and domestic firms may differ in their perspective towards the privacy of customers.³

The international firm which is well-known globally contains far greater detail when it comes to the kinds of personal information that is collected, the purposes for which it would be put and the period of retention. While the domestic firm pays considerable attention to how information is disclosed or shared, this still dwarves in comparison to the international firm. This pattern and difference of mention and detail can be seen with regard to the rights of data subjects as well. While the international

³ While this discussion may more organically belong in the section entitled ‘Discussion of empirical findings’, it is included here to depict the lack of standardization in the transport industry.

firm explains these rights in great detail, the domestic firm simply states that it will “...comply with individual’s requests regarding access, correction, and/or deletion of the personal data it stores in accordance with applicable law.”

Therefore, out of the four privacy policies related to the transport industry that are examined in this study (two of which contain very little detail) there is little to no standardization within the transport industry and great deviation between local and international firms. However, it is worth noting that the domestic firm in question drafted its privacy policy on the 1st of May, 2016 – 6 years before the Sri Lankan Data Protection Act was enacted and more importantly 2 years before the GDPR came into effect. No date is mentioned for when it was last updated while the international firm’s policy was updated last on the 13th of October, 2022. This goes to show that even before the GDPR came into being, some firms in Sri Lanka were, at least on paper, cognizant of the high standards of privacy enumerated in the GDPR and selected for comparison in this article in the section entitled ‘Level of acknowledgement of GDPR standards in local and international firms’.

In summary, contrary to the hypothesis, this section suggests that the privacy policies of firms are not standardized within industries. While there are similarities, there appear to be unique provisions for each firm. The implications of this for the design of privacy policies will be discussed later in this article.

Standardization across industries

Much like the lack of standardization within industries, there appears to be deviation across industries as well, although with some level of standardization. While this was proven with quantitative statistics, this section explains it further through the content of the terms. Given the different level of detail that is provided in each of the industries and individual firms, this section is cautious of making broad stroked generalizations. It attempts to adopt a more nuanced approach of acknowledging both differences within similarities as well as similarities within differences in order to refrain from arriving at false generalizations.

To begin with, the strongest privacy protections can be found in the cloud computing industry. However, when it comes to other industries, the same standards can be found in the policies that carry the strongest levels of protection. Therefore, in a sense, according to the level of protection, there is standardization across industries.

The strongest privacy policies in the banking, supermarket and transport sectors were able to match the protections that almost all the firms in the cloud computing industry contain.⁴ However, in these three industries, especially in the transport industry there were policies that fell far short of this standard.

⁴ It is important to note that this does not mean that the phrasing of the policies with the best protections are similar, but that they have a similar high level of consideration for consumer privacy.

When looking at the more mid-tier protections which are what can be seen in majority of the privacy policies in the banking,⁵ supermarket and transport sectors, they can be said to be similar in terms of standards of privacy. While there is likeness in how the terms are presented given that they all deal with almost the same kinds of protections and rights, a closer look shows that they look to be original stipulations of the standard privacy terms.

Finally, when it comes to the weakest protections that are provided by some policies, they cannot be said to be standardized in their ignorance but that they are non-compliant with international standards and practices.

Difference between terms in international and domestic firms

When comparing international and domestic firms, several interesting patterns emerge. Table 2 has been reproduced in a manner that it considers the international and domestic firms within each industry (see Table 3). At the outset, I acknowledge that considering only one cloud computing firm in Sri Lanka as well as one international transport firm that operates in Sri Lanka would be statistically problematic. However, I am compelled to continue with one firm for each category as they are the only firms that operate in Sri Lanka and contain privacy policies to the best of my knowledge.

Table 3: Level of compliance of domestic and international firms

	Cloud computing		Banking		Supermarket		Transport	
	Domestic N = 1	International N = 4	Domestic N = 3	International N = 2	Domestic N = 4	International N = 2	Domestic N = 3	International N = 1
Legal basis	100%	100%	100%	100%	100%	100%	66.67%	100%
Disclosure of purpose for processing data	100%	100%	100%	100%	100%	100%	66.67%	100%
Kinds of personal data processed	100%	100%	100%	100%	100%	100%	66.67%	100%
Period of retention	100%	75%	66.67%	100%	50%	50%	33.33%	100%
Data subject rights								
• Access	100%	100%	66.67%	100%	75%	100%	33.33%	100%
• Rectification	0%	100%	66.67%	100%	75%	100%	33.33%	100%
• Restriction	0%	100%	0%	100%	50%	0%	33.33%	100%
• Deletion/erasure	100%	75%	0%	100%	25%	50%	33.33%	100%
• Portability	0%	50%	0%	100%	25%	0%	0%	100%
Security	0%	100%	100%	100%	100%	50%	0%	0%
Sharing of data	100%	100%	66.67%	100%	100%	100%	66.67%	100%

⁵ This is except for the security provision which is at a higher level.

One pattern that is clear from the above data is that except for a few terms, in majority of the instances there appears to be higher incorporation of international standards of data privacy by international firms. This is especially so in the banking industry which shows complete cognizance of all the international standards in focus in the current study. This is followed by the transport industry and cloud computing industry which only falls slightly short with the former failing in reference to security and the latter in providing information on the retention of data, another one firm in right to erasure and two in right to data portability.

The supermarket industry appears to be a mix. International firms seem to carry quantitatively equal or higher levels of protection except for right to restrict data and security of data.⁶ However, qualitatively, it is difficult to draw conclusions since there are domestic firms with detailed and high standards of protection in the mix and vice versa.

The biggest deviation that can be found with Prof. Wurgler's conclusion with regard to US firms is that the one domestic firm in Sri Lanka [Company A] that provides cloud services does not appear to speak of the rights to rectification, restriction and erasure. The most glaring deviation, however, is that it does not guarantee absolute security, making domestic cloud computing firms quantitatively less protective of consumers' privacy than international firms. However, it is worth considering the possibility or rather impossibility of guaranteeing absolute security and the abilities of foreign firms to meet this standard regardless of it being mentioned so in their privacy policies.

Length of contracts in terms of space

The GDPR requires that information referring to the rights of data subjects as well as the principles relating to how the personal information of data subjects would be dealt with be provided “...in a concise, transparent, intelligible and easily accessible form, using clear and plain language” (GDPR, article 12).

This section looks at the brevity or lack thereof of privacy policies in the different industries while also looking at it from a comparative lens between domestic and international firms (Figure 1). The next section looks at the level of readability of the texts.

⁶ *Supra* section entitled ‘Empirical findings’.

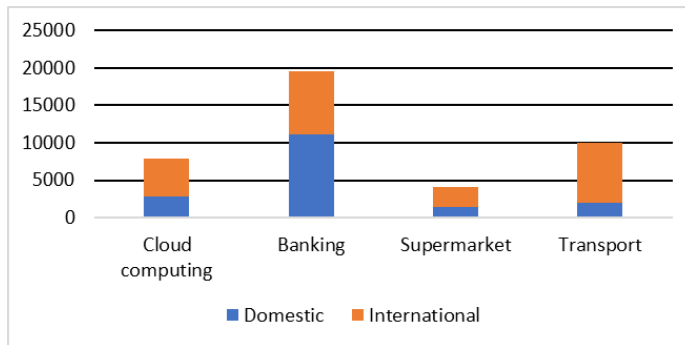


Figure 1: Average length of privacy policies in terms of word count

Apart from the banking industry, the international privacy policies in other industries appear to be longer than domestic policies. Most of them stretch on to around 3 – 10 pages with single-spaced Times New Roman font of 12 in English. The language of the privacy policies is important as their limitation to one language that is not spoken by majority consumers in Sri Lanka would have negative repercussions for the accessibility of the privacy policies. This is elaborated in the sub-section entitled ‘Readability of contracts’.

It is fair to conclude that there is greater cognizance of the requirement for brevity on the part of Sri Lankan firms than international firms. However, as the sections above depict, international firms provide greater levels of protection both qualitatively and quantitatively than local firms. To refer to more rights and heightened rights, the privacy policies may have to naturally use more space as it would usually incorporate a higher number of rights for data subjects and greater number of obligations for controllers and processors of data. Ironically though, in the banking sector, international firms appear to abide by all international standards that this study pays attention to and yet manages to be shorter than the average domestic privacy policy. The international firms’ policies in transport and cloud computing industries appear to be much longer in word count than local firms, but again claim compliance with a greater level of data protection principles. Finally, in the supermarket industry domestic and international firms offered mixed levels of protection which did not allow any decisive conclusions to be drawn. However, even in the mix of differing levels of protection being offered by firms, the length of international privacy policies appears to be much longer in terms of word count.

Readability of contracts

This section explores the readability of the contracts which is stipulated in the GDPR under article 12 which is required to be “*intelligible*” and in “*clear and plain language*.” To begin with, none of the contracts could be said to be free of ‘legalese’.

This is a term coined to mean complicated legal language (Butt, 2001) that is not easy to read. However, a stark exception can be found in one contract in company D cloud computing industry, which was one of the longest but was presented in a comparatively reader friendly way and contained videos that explained the rights of data subjects and privacy principles with attention grabbing animations. Apart from this one example, all the other contracts suffered from hindrances to readability to varying degrees.

In order to quantitatively measure readability, this study utilizes the Flesch-Kincaid reading ease and the Flesch-Kincaid grade level. The Flesch-Kincaid reading ease and the Flesch-Kincaid grade level look at the average number of words per sentence and average number of syllables per word in calculating the readability of a document (Sirico Jr., 208). The difference between the two is the different weightages that are attached in the formulae used for the two measurements. The higher the score on the Flesch-Kincaid reading ease test, the easier the text would be to read. Rudolf Flesch himself has ranked several reading materials according to his test and they may prove instructive in interpreting our findings (Table 4).⁷

Table 4: Flesch Reading Ease Score of different materials

Comics	92
Consumer ads in magazines	82
Movie screen	75
Seventeen	67
Reader’s Digest	65
Sports illustrated	63
New York Daily News	60
Atlantic Monthly	57
Time	52
Newsweek	50
Wall Street Journal	43
Harvard Business Review	43
New York Times	39
New York Review of Books	35
Harvard Law Review	32
Standard auto insurance policy	10
Internal Revenue Code	minus 6

⁷ Rudolf Flesch, How to Write Plain English, University of Canterbury https://web.archive.org/web/20160712094308/http://www.mang.canterbury.ac.nz/writing_guide/writing/flesch.shtml

To these values the Flesch-Kincaid tests attach a grade level based on US grading. Online sources identify grade levels to correspond to levels: basic (level 1 – 6), average (level 6 – 12) and skilled (level 12 – 18) (Flesch Reading Ease and the Flesch Kincaid Grade Level). The basic level is said to be at a standard to comprehend texts tackled by persons who are new to reading such as “Learning to read” and “The Gruffalo.” The average level includes books such as “Harry Potter” and “Jurassic Park”. Finally, skilled level comprises of texts such as “A brief history of time” and academic papers.

Important to note, however, is that the Flesch-Kincaid readability tests are far from perfect. They suffer from technocentrism along with other ills (Sirico Jr., 2008). However, there is no denying their usefulness in putting a number to the ability to read a text and these texts have been utilized in many contexts within the law (Sirico Jr., 2008).

Figures 2 and 3, depicted below, show the average Flesch-Kincaid reading ease level and the average Flesch-Kincaid grade level for each industry.

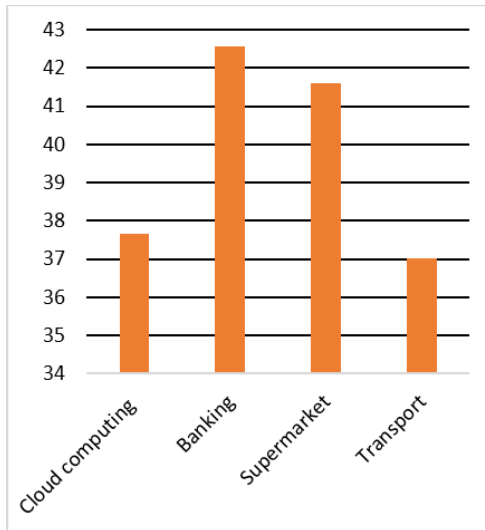


Figure 2: Flesch-Kincaid reading ease

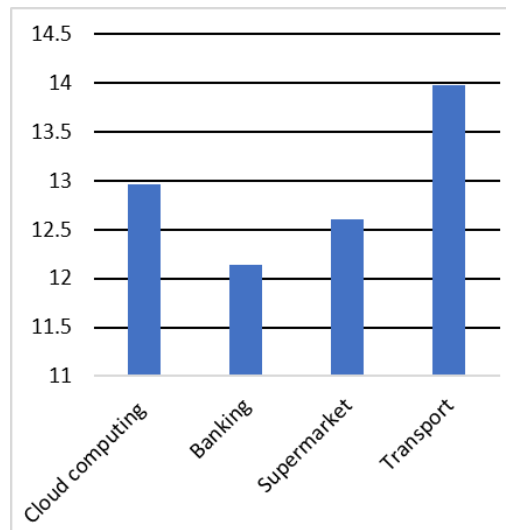


Figure 3: Flesch-Kincaid grade level

As the figures reveal, the reading ease level appears to range between 37.025 and 42.58. This is akin to reading articles in the Harvard Business Review, New York Times, and the New York Review of Books, all of which signal a substantially low level of readability. Almost all the contracts fall within the skilled level of above 12 which goes to substantiate that the readers of the privacy policies should have a very high standard of understanding. There is variation within the industries where the banking industry appears to have the easiest read, with supermarket, cloud computing and transport industries following respectively. However, the differences are negligible given that they all require high levels of reading skill.

It is important to note that these difficulties may be compounded in a linguistically diverse country such as Sri Lanka. The privacy policies that are drafted by these websites are in English. However, the official languages recognized by the Constitution of Sri Lanka are Sinhala and Tamil (Constitution, Art. 18). English is not the first language of majority Sri Lankans and in fact, only 15% Sri Lankans speak English (Sittarage, 2018). Among the 15% that can speak the language, proficiency would be at differing levels. Therefore, these privacy policies would be all the more difficult for Sri Lankan consumers to read and understand making them more inaccessible for a greater portion of consumers in the country.

Discussion of empirical findings

In analyzing the above findings, I repeat the questions we had at the very beginning - when companies do not face binding legal obligations, do they draft privacy policies in line with international standards? To what extent are privacy terms standardized within and across industries? To what extent do the firms want to give the impression that they care about the privacy of their customers, and do they make their privacy policies concise and readable for the benefit of their consumers? This article does not answer all these questions in the affirmative. It both satisfies and falls short of satisfying GDPR-level protections with possibilities to increase alignment with such high standards. A value judgment on whether it is a good practice to align with GDPR level of data privacy protection is beyond the scope of this article.

To begin with the level of incorporation of international privacy standards in privacy policies, majority of enterprises across all industries, except domestic transport services, appear to be cognizant of said standards. This contrasts with the hypothesis of the study which was critical of the attention that especially domestic firms pay to the data privacy of their consumers. Given that most of the policies do not contain information as to when it was last updated, it is difficult to assess their awareness of the local law – the PDPA. The only contract in Sri Lanka that acknowledges this law is largely in line with it. The few other policies that contained a date on which it was last updated were before the local law was enacted. Therefore, in a context where there is no compulsion to come in line with international standards, there is a clear attempt on the part of majority of the firms to do so. This goes to show that, at least to an extent, firms that operate in Sri Lanka do keep in mind international standards, here in the form of the GDPR, when designing their privacy policies that lay out their obligations regarding the data privacy of their consumers.

The fact that there is little standardization within firms in the industry is also telling of the way these policies are designed. However, this could be interpreted in different ways. For one, the lack of standardization might signal that firms put in time and effort in drafting their own privacy policies on their own terms while largely staying in line with recognized international practices. No privacy policy, even those

in the transport industry, which have relatively lower protection appeared to be carbon copies of terms in the contracts of other firms. However, a second possibility might be that the lack of standardization is due to the absence of an established culture of privacy within the industries and the country. This, however, may not be the case as even foreign firms that contain high protections stipulate their terms in unique ways. A third possibility for the deviation between firms might be because they are unwilling to take on additional responsibilities when they are not required to and therefore purposefully refrain from mentioning the relevant obligations or draft them in such a way that they do not encompass the full breadth of the responsibility as laid out in the GDPR. However, the mere mention of the right or principle might still be enough for consumers to enforce the full gamut of what the right entails. As when disputes arise in courts with regard to violations of data privacy rights, the mere mention of the right of the consumers in the policies, absent further elaboration, would allow judges to look to other jurisdictions in interpreting the right and enforcing it in a broad manner to ensure greater protection for the personal data of consumers, should they choose to. There is minimal uniformity in the level of detail that firms incorporate, on the part of both local and international firms when it comes to rights of data subjects and principles of data protection. However, their very existence in the contracts bodes well for consumers that enjoy these services. While the lack of standardization might be for any of the above reasons and more, one thing that is undeniable is that when designing privacy policies, companies prefer to draft their own terms as opposed to relying on privacy boilerplates.

Regarding the level of standardization across industries, overall, much like Prof. Wurgler's study where there was found to be greater privacy protection for cloud computing sites and adult sites, here too there is higher protection on average in the cloud computing industry and banking industry. This makes sense as these industries deal with highly sensitive information. This, however, would clash to an extent with the finding that the Sri Lankan firm that provides cloud services fails to stipulate absolute guarantee of security of the personal information and some other data subjects' rights. While the lack of terms that lay out security features that are implemented does not necessarily mean none are available, the lack of its mention signals less attention being paid to transparent communication to consumers of the safety and confidentiality of important details that may be used to identify them.

There is a lower level of attention both quantitatively and qualitatively in the privacy policies of the local transport industry but this is understandable due to the lack of local legal obligation pertaining to personal information of consumers. However, given that there is highly sensitive information such as financial details that are saved in these applications when taking trips and ordering food, it is alarming that more attention is not paid to ensure the protection of personal information of its clients. I concede that financial information is not considered to be sensitive information by

either the PDPA or the GDPR. However, for one this study considers the status of privacy policies regardless of the coming into effect of the former law. Further, since under financial information I consider data such as credit card numbers that one enters when receiving transport services, these would be important due to the sheer impact they have on a person's economic circumstances if not properly protected. It comes as no surprise that compared to the local firms, the international firm sets very high standards of privacy, especially given its global popularity. However, what does not fit in the narrative is that this international firm does not contain a provision guaranteeing or setting out the measures that the company resorts to, to safeguard the personal information of data subjects.

It is, therefore, fair to speculate that market forces play a part in the design of privacy policies in certain industries, but perhaps it should not be so given that all four of these industries contain sensitive information that consumers would similarly wish to maintain control over.

Another finding that we encountered above is that for most of the industries, the international firms were providing higher consumer privacy protection. This is to be expected since companies that are already abiding by higher privacy standards for certain countries that would be governed by the GDPR or other laws that contain obligations that are as strict as the GDPR, it would make little sense to tailor its practices to countries that would not enjoy such high levels of protection. The tailoring itself may take more resources than the consistent application of practices that have already been brought in line with the world's strictest privacy regulation. Not to mention, this may also be used by firms to gain a competitive edge by branding themselves as more cognizant of the privacy of its consumers. Moreover, the greater reputations and higher resources undoubtedly aid these firms in developing legal compliance, regardless of the jurisdiction they function in.

It is worth mentioning however, that there are local firms that are just as comprehensive and privacy minded as international firms, although when averaged they may not seem so. The opposite also holds true as there are some international firms, in the supermarket and cloud computing industries, that do not guarantee certain principles and rights of data subjects.

Overall, however, it is reasonable to suggest that privacy policies are less likely to be designed in line with international standards if it is not mandatory. Moreover, there is higher likelihood that when certain firms that operate in jurisdictions that are governed by international standards such as the GDPR, this would be maintained consistently regardless of the presence of such regulations in other countries of business.

Finally, there is much to strive for both local and international firms in making their privacy policies concise and readable for the benefit of their respective consumers. This is further compounded by the fact that English is not the first

language of many Sri Lankans (Sittarage, 2018), making these privacy policies less accessible for the majority. Therefore, it is fair to suggest that the consumer that is expected to benefit from the publication of these privacy policies is not kept in mind when they are drafted to be as long and as difficult to read as they are.

However, to ignore the flip side would do the debate a great disservice. While the length of international firm privacy policies was greater than that of local firms on average, we must also keep in mind that the longer contracts, as can be seen in the international firms in the cloud computing industry, contained more information, better presentation, and greater rights for consumers. To sacrifice that for the sake of brevity would not be a solution. However, the banking industry is a good example of how brevity does not always have a converse relationship to the level of protection. With regard to the readability of the contracts, it is important to keep in mind that these contracts may set out binding legal obligations and notice. Therefore, the allure in resorting to the known legal jargon cannot be denied. However, if these policies were to be drafted for the benefit of the consumer, changes would need to be made.

Conclusion

To conclude, this study finds that out of the firms that operate in Sri Lanka, both international and local, in the areas of cloud computing, banking, supermarket and transport, there is recognition of international legal principles even absent legal compulsion. Standardization within and across markets is minimal. The international firms appear to offer greater protections than local firms, but the flipside is also true in some cases. We also saw that the contracts are long and difficult to read. These findings lead us to the conclusion that while the recognition of privacy may not have been as poor as hypothesized, there is much that needs to be kept in mind in designing contracts that set out the privacy practices of companies regarding the personal information of their consumers. Greater acknowledgement of the standards within a heightened culture of privacy in a more concise and readable format would help bring the privacy policies of Sri Lanka in line with international standards and guarantee greater protection for the privacy of consumers of the country.

Conflict of Interest

The author has no conflict of interest to declare.

References

- Allyson W. Haynes. (2007). Online Privacy Policies: Contracting Away Control Over Personal Information?, 111 *DICK. L. REV.* 587 (2007). <https://ideas.dickinsonlaw.psu.edu/dlra/vol111/iss3/3>
- Bareh, C. K. (2021). Assessment of the privacy and security practices of the Indian academic websites. *Library Philosophy & Practice* (e-Journal), 6426

- Brown, J. D., Ghani, M. A., Hoque, M., & Rehman, U. A. (2012). An Analysis of Web Privacy Policies Across Industries. *Worcester Polytechnic Institute*
- Butt P., June/July 2001 'Legalese versus plain language' *Amicus Curiae* 35
- Buttarelli G. (2016). The EU GDPR as a Clarion Call for a New Global Digital Gold Standard. *International Data Privacy Law*, 6(2), 77
- Chatsuwan, P., Phromma, T., Surasvadi, N., & Thajchayapong, S. (2023). Personal data protection compliance assessment: A privacy policy scoring approach and empirical evidence from Thailand's SMEs. *Heliyon*, 9(10)
- Constitution of the Democratic Socialist Republic of Sri Lanka (1978)
- Degeling, M., Utz, C., Lentzsch, C., Hosseini, H., Schaub, F., & Holz, T. (2018). We value your privacy... now take some cookies: Measuring the GDPR's impact on web privacy. arXiv preprint arXiv:1808.05096.
- EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC
- Fernando J. & Wickramasinghe S. (2022). Sri Lanka Personal Data Protection Legislation – An Overview. <https://ssrn.com/abstract=4246818> or <http://dx.doi.org/10.2139/ssrn.4246818>
- Flesch R. How to Write Plain English, University of Canterbury. https://web.archive.org/web/20160712094308/http://www.mang.canterbury.ac.nz/writing_guide/writing/flesch.shtml
- Flesch Reading Ease and the Flesch Kincaid Grade Level. <https://readable.com/readability/flesch-reading-ease-flesch-kincaid-grade-level/>.
- Javed, Y., Salehin, K. M., & Shehab, M. (2020). A study of South Asian websites on privacy compliance. *Ieee Access*, 8, 156067-156083
- Jensen C. & Potts C., (2004). Privacy Decision-Making Tools: An Evaluation of Online Privacy Notices, *CHI* 24-29, Vienna, Austria
- Jiang, Y., & Syn, T. (2023). Online privacy policy disclosure: an empirical investigation. *Journal of Computer Information Systems*, 63(3), 663-680
- Mantelero A. (2020). The Future of Data Protection: Gold Standard vs. Global Standard. *Computer Law & Security Review* 40. 105500. 10.1016/j.clsr.2020.105500
- Maraba, J., & Da Veiga, A. (2023, October). A Study of Online Privacy Policies of South African Retail Websites. In International Conference on Advanced Research in Technologies, Information, Innovation and Sustainability (pp. 426-440). Cham: Springer Nature Switzerland. https://link.springer.com/chapter/10.1007/978-3-031-48855-9_32
- Marotta-Wurgler, F. (2016). Self-Regulation and Competition in Privacy Policies. *The Journal of Legal Studies*, 45(2)

- Marotta-Wurgler, F. (2016). Understanding privacy policies: Content, Self-Regulation, and markets. *NYU Law and Economics Research Paper No. 16-18* <https://doi.org/10.2139/ssrn.2736513>
- McDonald, A. M., Reeder, R. W., Kelley, P. G., & Cranor, L. F. (2009, August). A comparative study of online privacy policies and formats. In *International Symposium on Privacy Enhancing Technologies Symposium*, 37-55. Berlin, Heidelberg: Springer Berlin Heidelberg
- Neethling, J., Potgieter, J. M., & Visser, P. J., (2005). *Neethling's Law of Personality*. (2nd Edition). LexisNexis Butterworths
- Norton, T. B. (2016). Thomas B. Norton, The Non-Contractual Nature of Privacy Policies and a New Critique of the Notice and Choice Privacy Protection Model, 27 *Fordham Intell. Prop. Media & Ent. L.J.* 181 <https://ir.lawnet.fordham.edu/iplj/vol27/iss1/5>
- Nokhbeh Zaeem, R., & Barber, K. S. (2017). A study of web privacy policies across industries. *Journal of Information Privacy and Security*, 13(4), 169-185
- Nyshadham, E. A. (2000). Privacy policies of air travel web sites: a survey and analysis. *Journal of Air Transport Management*, 6(3), 143-152
- Personal Data Protection Act No. 9 of 2022 (Sri Lanka)
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) (OJ L 119 04.05.2016, p. 1, ELI: <http://data.europa.eu/eli/reg/2016/679/oj>)
- Sirico Jr. L. J. (2008). Readability Studies: How Technocentrism Can Compromise Research and Legal Determinations. *Working Paper Series, Villanova University Charles Widger School of Law*
- Sittarage N. (2018). English Language Education in Sri Lanka Link with the Learners Motivational Factors. *Humanising Language Teaching*, 20(4) <https://www.hltmag.co.uk/aug18/english-language-education-in-sri-lanka>
- Taylor M. (2020). Data protection: threat to GDPR's status as 'gold standard'. *International Bar Association*. <https://www.ibanet.org/article/A2AA6532-B5C0-4CCE-86F7-1EAA679ED532>
- Zaeem, R. N., & Barber, K. S. (2020). The effect of the GDPR on privacy policies: Recent progress and future promise. *ACM Transactions on Management Information Systems (TMIS)*, 12(1), 1-20