scripted

Volume 5, Issue 3, December 2008

The Right to Privacy in the Information Era: A South Asian Perspective

Althaf Marsoof[*]

Abstract

The famous saying that "Your freedom ends where my nose begins"[1] *may, in the electronic era, be transformed to mean "Your freedom ends where my 'Network' begins". The progression into an e-literate society in which the electronic medium is used to transact all forms of business – including government (e-governance) – has greatly increased the need to protect the privacy of the individual from invasions not only by the State, but also from others who seek to profit from such intrusions. This paper probes into the latest trends in modern technology and analyses the existing legal framework in Sri Lanka and India in support of the argument that the right to privacy must be guarded as a constitutional right.*

DOI: 10.2966/scrip.050308.553

---

[*] B.Sc. (Curtin University of Technology), Attorney-at-Law. The author is a State Counsel in the Attorney General's Department of Sri Lanka and is also a Visiting Lecturer in Business and Computer Law at the Sri Lanka Institute of Information Technology.

[1] Legislative Assembly of Ontario, Canada: Parliamentary debate on the *Advocacy Bill of 1981*. Hansard available at http://www.ontla.on.ca/hansard/committee_debates/35_parl/session1/justice/j069.htm.

1. Introduction

Article 12 of the Universal Declaration of Human Rights enunciates that "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attack upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks".[2] Many jurisdictions across the globe including South Korea,[3] Spain,[4] Switzerland,[5] Thailand[6] and the United Kingdom[7] have recognised privacy as a fundamental right. In fact, the right to privacy forms an important part of the Common Law tradition, which has considerable influence in Sri Lanka, India and most other South Asian nations by reason of their colonial heritage. The Common law approach is reflected in the following words of Sir William Pitt, the Earl of Chatham, which are often quoted:

> *The poorest man may in his cottage bid defiance to all the force of the Crown. It may be frail; its roof may shake; the wind may blow through it; the storms may enter, the rain may enter, - but the King of England cannot enter; all his forces dare not cross the threshold of the ruined tenement!*[8]

Privacy undoubtedly connotes a very important personal right, and thus if one's privacy is to be disturbed it ought to be done with good reason and constraint. With the advent of telecommunication and now the internet, e-commerce and e-governance, privacy has attracted much attention.

This paper delves into an analysis of the present legal regime in Sri Lanka, in relation to privacy as a right and a tool to protect human dignity and esteem; especially in the light of the new developments in Information Communication Technology (ICT). Modes by which one's privacy can be encroached upon through the use of modern technology will also come into focus in this paper. Privacy has often been looked upon as an individual right, which fails to consider the broader aspect of privacy as a social right. The failure to do so generates difficulty in striking a fine balance with competing social interests such as, for example, national security. Hence, in this paper, the social implications of the right to privacy will be considered with a view to building a stronger case for providing constitutional protection for privacy – especially in the context of the modern evolution towards e-governance.

---

[2] Adopted by the General Assembly of the United Nations on 10 Dec 1948.

[3] Articles 16, 17 and 18 of the *South Korean Constitution*.

[4] Article 18 of the *Constitution of the Kingdom of Spain*.

[5] Article 36(4) of the *Constitution of Switzerland 1874* and Article 13 of the *Public Referendum in April 1999*.

[6] Section 34 of the *Constitution of Thailand 1997*.

[7] *Human Rights Act 1998 (UK)*.

[8] William Pitt, Earl of Chatham, Speech on the Excise Bill in Bartletts, *Familiar Quotations* (10th ed., 1919). See also *Entick v Carrington*, 95 ER 807, [1765] 2 Wils. KB 275.

2. What is "Privacy"?

Privacy is a difficult term to define as its definition and scope are largely shaped by the culture and social norms of a country or region. However, certain general ideas have been put forward by numerous jurists, some of which are noteworthy.

One of the earliest views was that of Justice Louis Brandeis of the United States Supreme Court who articulated that the concept of privacy was the individual's "right to be left alone".[9] A more comprehensive and pragmatic view has been offered by Alan Westin, author of *Privacy and Freedom*, who defines privacy as "the desire of people to choose freely under what circumstances and to what extent they will expose themselves, their attitudes and their behaviour to others".[10]

In Sri Lanka, as well as in other neighbouring countries such as India, privacy has not been recognised as a constitutional right. Consequently, the courts have endeavoured to draw a balance between this individual right and the welfare of the public at large – especially when national security is in peril. Thus, there is a rich resource of case law that one could look into to analyse the proactive role played by the judiciary in protecting privacy as a human right without distressing national security. Of course, with the evolution of the internet and the electronic world, the courts have been invited to deal with situations that were never envisaged by it or by legislators. It is therefore useful to consider the present legal framework in Sri Lanka and India concerning privacy and its implications.

3. The Right to "Privacy" in India and Sri Lanka: A Comparison

Chapter III of the Constitution of Sri Lanka (1978) is silent as to a right to privacy. Similarly the Indian Constitution does not expressly guarantee a right to privacy. Therefore, on the face of it, it may seem that the law both in India and Sri Lanka has placed less emphasis upon this right. Several judicial pronouncements warrant examination at this juncture.

To begin with, the Indian Supreme Court did not avail of the opportunity to impute a constitutional element of privacy in *M.P. Sharma and Others v Satish Chandra, District Magistrate, Delhi and Others*[11] and went on to observe that:

> *When the Constitution makers have thought fit not to subject such regulation to constitutional limitations by recognition of a fundamental right to privacy, analogous to the American Fourth Amendment, we have no justification to import it, into a totally different fundamental right, by some process of strained construction.*

Though, initially, the Indian courts took a stringent stance against regarding the right to privacy as a fundamental right, with the passage of time a more liberal approach

---

[9] S Warren and L Brandeis, "The Right to Privacy" (1891) 4 *Harvard Law Review*, 193-220.

[10] A Westin, *Privacy and Freedom*, Atheneum 7.

[11] *M P Sharma and Others v Satish Chandra, District Magistrate, Delhi and Others*, AIR 1954 (SC) 300.

was taken and perhaps the landmark decision of *Kharak Singh v The State of Uttar Pradesh and Others*[12] is a manifestation of this change in judicial thinking. However, it must be pointed out that the Indian courts were not willing to expressly recognise a fundamental right to privacy. This becomes apparent from the words of Justice Subba Rao in *Kharak Singh*, which are as follows:

> *Further, the right to* personal liberty *takes in not only a right to be free from restrictions placed on his movements, but also free from encroachments on his private life. It is true our Constitution does not expressly declare a right to privacy as a fundamental right, but the said right is an essential ingredient of personal liberty. Every democratic country sanctifies domestic life; it is expected to give him rest, physical happiness, peace of mind and security. In the last resort, a person's house, where he lives with his family, is his "castle": it is his rampart against encroachment on his personal liberty. The pregnant words of that famous Judge, Frankfurter J., in* Wolf v. Colorado*, (1949) 338 US 25, pointing out the importance of the security of one's privacy against arbitrary intrusion by the police, could have no less application to an Indian home as to an American one.*

In *Rajagopal alias R.R. Gopal and another v State of T.N. and others*,[13] the Indian Supreme Court held that the right to privacy is not enunciated as a fundamental right in the Indian Constitution but may be inferred from Article 21.[14] In this case, reliance was placed on *Kharak Singh* and other decisions of English and American courts for holding that the petitioners had a right to publish what they alleged to be an autobiography of A. Shankar (insofar as it appears from the public records), even without his consent or authorisation. The Court however cautioned that, if they go beyond that and publish his life story, they may be invading his right to privacy. For this purpose, the Court held that a citizen has a right to safeguard his own privacy, as well as that of his family, marriage, procreation, motherhood, child-bearing and education among other matters. No one can publish anything concerning the above matters without his consent, whether truthful or otherwise and whether laudatory or critical. The position may, however, be different if a person voluntarily thrusts himself into controversy or invites or raises a controversy. The Court also pointed out an exception to such an instance, namely:

> *This is for the reason that once a matter becomes a matter of public record, the right to privacy no longer subsists and it becomes a legitimate subject for comment by press and media among others. We are, however, of the opinion that in the interests of decency [Article 19(2), Indian Constitution] an exception must be carved out to this rule, viz., a female who is the victim of a sexual assault, kidnap, abduction or a like offence should not further be subjected*

---

[12] *Kharak Singh v The State of Uttar Pradesh and Others*, AIR 1963 (SC) 1295.

[13] *Rajagopal alias R.R. Gopal and another v State of T.N. and others*, AIR 1995 (SC) 264.

[14] No person shall be deprived of his life or personal liberty except according to procedure established by law.

> *to the indignity of her name and the incident being published in press/media.*[15]

Therefore, it is clear that the Indian judiciary has inferred an implied right to privacy in the guise of "personal liberty" which is protected in terms of Article 21 of the Indian Constitution.

Of course, drawing the balance between privacy and the right to information has been a daunting task as these rights are repellent in nature. In fact, in certain instances the law has permitted intrusions into privacy, subject to carefully formulated safeguards. For instance, the Right to Information Act of India,[16] which provides

> *...for setting out the practical regime of right to information for citizens to secure access to information under the control of public authorities, in order to promote transparency and accountability in the working of every public authority, the constitution of a Central Information Commission and State Information Commissions and for matters connected therewith or incidental thereto.*

In Section 8(1) of the same Act, it is enacted that:

> *Notwithstanding anything contained in this Act, there shall be no obligation to give any citizen,*
>
> *(j) information which relates to* personal information *the disclosure of which has no relationship to any public activity or interest, or which would cause* unwarranted invasion of the privacy *of the individual unless the Central Public Information Officer or the State Public Information Officer or the appellate authority, as the case may be, is satisfied that the larger public interest justifies the disclosure of such information*

This statute clearly establishes that even the right to information is very much restricted when it comes to personal liberty and privacy. It is only applicable to the inspection of activities in the public sector and not in other situations.

Across the Palk Strait, the Constitution of Sri Lanka, in its chapter on Fundamental Rights, not only fails to expressly secure the right to privacy of citizens but also, unfortunately, does not contain a provision similar to that of Article 21 of the Indian Constitution.[17] Therefore, the Sri Lankan courts are confronted with a serious problem in upholding the right to privacy of individuals and it is interesting to examine how courts have overcome this difficulty.

Privacy issues have arisen in Sri Lankan courts in several contexts, ranging from servitudes, criminal trespass, divorce and defamation to unlawful arrest. In a case in the early-twentieth century, the court recognised a right to household privacy in

---

[15] See note 13.

[16] *Right to Information Act No 22 of 2005 (India)*.

[17] Article 13 of the Sri Lankan Constitution safeguards "personal liberty". However, it is applicable only to the arrest and custody of persons.

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.[18] It is noteworthy that the Sri Lankan courts have been bold to hold that even an owner of an estate or a superintendent has no right to enter the labourer's lines and invade his privacy.[19] The Supreme Court of Sri Lanka, in an appeal from a magistrate's court where a husband and wife had been convicted[20] of insulting several police officers who had entered their house on suspicion that they were in possession of stolen goods, 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, also, where the *privacy* and sleep of the accused appellant were disturbed).[21]

However, it must not be forgotten that in the midst of pressure from the media and the public for more transparency (especially in relation to alleged corruption in the public sector), the Sri Lankan courts have managed to strike a fine balance between the freedom of expression as guaranteed by Article 14(1)(a) of the Sri Lankan Constitution and the right to privacy. In fact, on numerous occasions, our courts have extended the right of publication and expression to engulf the right to information and the right to know. It is in this light that one must ponder upon the seminal judgment of Justice Hector Yapa (the President of the Court of Appeal (as he then was); with Justice Kulathilake agreeing) in the infamous *Sunday Times* case.

This case (reported as *Sinha Rathnathunge v. The State*),[22] added new dimensions to the law relating to privacy in Sri Lanka. In this case, the appellant, the editor of the Sunday Times newspaper, was indicted on two counts under Section 480 of the Penal Code and Section 15 of the Sri Lanka Press Council Law.[23] The party defamed was Her Excellency the President of Sri Lanka. The appellant was found guilty on both counts.

In dismissing the appeal, the Court of Appeal observed that the right to privacy ought not to be impinged in the guise of a constitutional right of expression and publication. According to Justice Hector Yapa:

> *What the press must do is to make us wiser, fuller, surer, and sweeter than we are. The press should not think they are free to invade the privacy of individuals in the exercise of their constitutional right to freedom of speech and expression, merely because the right to privacy is not declared a fundamental right of the individual.*[24]

---

[18] *Chinnappa et al. v Kanakar et al.*, 13 NLR 157, at pages 158, 159 and 160.

[19] *Abraham v Hume*, 52 NLR 449, at page 453.

[20] Under sections 484 and 486 of the *Penal Code Act No 50 of 1980*.

[21] *A.M.K Azeez v W.T Senevirathne (SI Polce)*, 69 NLR 209, at page 210.

[22] *Sinha Ratnatunga v The State*, [2001] 2 SLR 172.

[23] *Sri Lanka Press Council Law No 5 of 1973*.

[24] See note 22, at page 212.

Further it was observed by his Lordship that every human has a "right to remain in society as a human being with human dignity".[25]

His Lordship, while striking a balance between the competing rights of privacy and freedom of expression, further observed that:

> *The law of defamation both civil and criminal is also geared to uphold the human being's right to human dignity by placing controls on the freedom of speech and expression. The press should not seek under the cover of exercising its freedom of speech and expression make unwarranted intrusions into the private domain of individuals and thereby destroy his right to privacy. Public figures are no exception. Even a public figure is entitled to a reasonable measure of privacy. Therefore Her Excellency the President even though she is a public figure is entitled to a reasonable measure of privacy to be left alone when she is not engaged in the performance of any public functions. That is a no entry zone which the press must not trespass. The case in hand is one where the press has attempted to enter into that no entry zone.*[26]

Therefore, from the above observation of Justice Yapa, it is manifest that the remedy against a breach of individual privacy is found in the Roman Dutch law (which is the common or residuary law of Sri Lanka) in the form of an action for injury under the *actio injuriarum*.[27] However, it must be noted that this action is very restrictive as many requirements have to be satisfied to succeed in a claim. This resulted in greater recourse to the criminal defamation provisions of the Penal Code.[28] However, the law imposing criminal sanctions for defamation was repealed by legislation enacted in 2002.[29] Thus, the law presently only recognises a civil remedy for defamation.

Hence, unlike in India, the right to privacy in Sri Lanka does not enjoy a constitutional backing. However, a remedy for violation of privacy does exist in the common law of Sri Lanka and may be used in appropriate instances. Thus, it may be concluded that the judicial wave that was triggered in India has not yet reached the shores of Sri Lanka with full force. Instead, we see the Sri Lankan jurisprudence in relation to privacy embedded in our common law; nourished by the creativity and innovation of our judges.

---

[25] See note 22, at page 213.

[26] See note 22, at page 213.

[27] See C Amarasinghe, *Aspects of the Actio Injuriarum in Roman-Dutch Law* (Colombo, 1966) - *The actio injuriarum* may be termed as an action for damages under the Roman-Dutch Law for loss of reputation and dignity.

[28] *Penal Code Act No 50 of 1980*.

[29] *Penal Code (Amendment) Act No 12 of 2002* and the *Press Council (Amendment) Act No 13 of 2002*; These pieces of legislation were enacted as a package to repeal the provisions that recognised defamation as a criminal offence. The Bills were passed by Parliament on 18 June 2002. The civil law remedy for defamation will continue to be available.

4. The Electronic World: "Privacy" at Stake!

Following the advent of electronics, the world has become a smaller place. The invention of the telephone was a momentous step towards the "e-globe". It may comfortably be said that all other developments were founded on telecommunication technology and thus, the telephone is the foundation of modern-day ICT. Law had to be moulded to meet the changes brought about by these inventions.

The advantage of using modern communication devices is that transfer of information is possible without confronting obstacles such as distance and time. At the same time, the possibility of information or *data* being intercepted and being placed in the hands of unintended parties has also increased. It is for this reason that privacy has become an issue in the context of electronic devices, communication and data transmission. Therefore, the need for stringent laws protecting personal data cannot be understated.

5. Are "Privacy" and "Data Protection" Two Distinct Concepts?

The meaning of privacy has already been dealt with. However, with view of answering the question as to whether privacy is a distinct concept from data protection it is first necessary to define *data*. One of the most comprehensive definitions of "data" is found in the Information Technology Act of India[30] (in Section 2(o)), which provides the following definition:

> ...data *means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer.*

Thus, data protection means the protection of information that can be generated using computer systems, as defined above.

Privacy is generally said to have four aspects; which are namely:

> **Information privacy**, which involves the establishment of rules governing the collection and handling of personal data such as credit information, and medical and government records. It is also known as "data protection";
>
> **Bodily privacy**, which concerns the protection of peoples' physical selves against invasive procedures such as genetic tests, drug testing and cavity searches;
>
> **Privacy of communications,** which covers the security and privacy of mail, telephones, e-mail and other forms of communication; and
>
> **Territorial privacy**, which concerns the setting of limits on intrusion into the domestic and other environments such as the workplace or

[30] *Information Technology Act No 21 of 2000 (India)*.

> public space. This includes searches, video surveillance and identity checks.[31]

Therefore, it is obvious that data protection is an aspect of privacy. Thus, a comprehensive legal regime that protects the right to privacy is important in the context of the electronic world.

6. Recent Trends

To discover modes in which privacy may be breached by the use of new technology, it is important to do a survey of the recent past – unravelling the developments in Information Technology (IT) and how the law has reacted to the ever-increasing privacy risk. The variables of "new technology" and "privacy risk" are "directly proportional" in mathematical terms. In other words, the development of ICT has correspondingly increased the potential to invade privacy.

The latest trend in IT is to provide faster and easier access to information, through connection media such as the internet. This has led to the introduction of various devices ranging from personal computers, laptops, palmtops and, of course, mobile phones which facilitate access to information.

There are a number of developments that are important and need consideration. They are:

> **Globalisation,** which removes geographical limitations to the flow of data. The development of the Internet is perhaps the best-known example of a global technology;
>
> **Convergence,** which is leading to the elimination of technological barriers between modern information systems; and
>
> **Multimedia,** which fuses many forms of transmission and expression of data and information gathered in a certain form that can be easily translated into other forms.

7. Globalisation, Convergence, Multimedia and ICT

Information Communication Technology (ICT) encompasses the full range of the production, distribution, and consumption of information, across all media from radio and television to satellites and the internet. It was the shift from analogue to *digital* technologies that triggered the convergence of computers, telecommunications, television, and the internet into a single multimedia environment. These are typically accompanied by important organisational and commercial changes as well. IT and the IT revolution refer not only to traditional communication functions, but also to the steady introduction of computer technology (in the form of microchips) and other hardware into nearly every sector and activity (including health, transport and education, to name a few). If the internet, computers and other communication

---

[31] *Privacy and Human Rights 2001: An International Survey of Privacy Laws and Developments* published by the Electronic Privacy Information Centre, Washington DC, USA.

devices are described as "pipes", then what flows through these *pipes* are data. The mode[32] in which these data are transmitted is known as *Multimedia*.

These developments mean that nations cannot remain isolated. Perhaps such isolation would lead to their destruction. The world has become a *global village* and this is made possible due to trans-border data interchange. Email is a very simple and effective example to illustrate this concept. In fact, local and international transactions have given rise to several legal complexities – especially in determining the jurisdiction of courts and the applicability of laws. It may reasonably be argued that the sovereignty of States have become blurred because of the internet. It is clear that ICT and globalisation – with the aid of multimedia and convergence – have opened gates to a wide array of possible ways by which information privacy may be invaded. From the perspective of privacy, this trend is dreadful. The need for extensive laws regulating information flow is currently being more readily felt in Sri Lanka than ever before.

8. Some Aspects of Modern Technology and the Corresponding Developments in the Law

The above investigation of the *recent trends* has led us to the irresistible conclusion that modern technology is vulnerable to privacy invasion. There are many modes in which information can fall into the undesired hands of inquisitive persons. However, this being a very broad area, this paper would focus on the most commonly used technologies.

8.1. Telecommunication

Homes and Offices around the globe are connected by telephones through a Public Switch Telecommunications Network. In simple terms, it is a grid of cables that connects every point in the network through portals known as "Gateways". This, in itself, provides great opportunities for information theft which is commonly known as "Telephone-Tapping". It may be apt to quote the words of Justice Kuldip Singh of the Indian Supreme Court, from a recent judgment concerning telephone tapping:[33]

> *Telephone-Tapping is a serious invasion of an individual's privacy. With the growth of highly sophisticated communication technology, the right to hold telephone conversation, in the privacy of one's home or office without interference, is increasingly susceptible to abuse. It is no doubt correct that every Government, howsoever democratic, exercises some degree of* sub rosa *operation as a part of its intelligence out-fit but at the same time citizen's right to privacy has to be protected from being abused by the authorities of the day.*

As far as Sri Lanka is concerned, it is a relief to note that the Telecommunication Act[34] provides for protection of data and regulates the interception of telephone

---

[32] Audio, visual or both.

[33] *People's Union of Civil Liberties v Union of India*, AIR 1997 (SC) 568.

[34] *Telecommunications Act No 27 of 1996*.

communications. According to Sections 53 and 54(1) of this Act, the interception of telecommunication transmissions and the disclosure of their contents is an offence subject to penalties including imprisonment. Until 2007, the only legislation that provided for some protection of data was the Telecommunications Act, and even the recently enacted Electronic Transactions Act[35] does not contain any provisions for data protection. The Sri Lankan Computer Crimes Act No 24 of 2007 introduced a comprehensive legislative framework to protect computer users from unauthorised access to computers and unlawful interception of data.

8.2. The Internet

The internet is a network of networks linked with millions of computers worldwide for communication purposes. The internet is a medium through which people can access information stored in other computers linked to the internet.[36]

Any computer connected to the internet can access any other linked computer and *vice versa* (provided permission and necessary access is granted by the computer owners). For example, if A's computer is linked to the internet and A wishes to share certain files in his computer with others, A may grant access to these files to other users of the internet. A can also grant access to only one or a group of computer users by employing network restrictions. A can also prevent others from forcing access to A's computer by installing appropriate firewalls and internet security software. Nevertheless, the very objective of the internet is to provide information access and sharing. This is a hacker's idea of heaven.[37] Let us examine a few ways in which privacy can be breached through internet usage.

8.2.1. The "Cookie" Crumbles

A cookie is not as sweet as it sounds. A cookie is a simple text file that will be discretely placed in the computer's hard disk when it gains access to certain websites. It stores information about the user. For example, it may store certain preferences shown by the user, such as: which part of the website the user frequently accesses; the time spent in these websites; or the user's preferred content. These are usually known as "clickstream data".[38] The methodology by which websites gather such information may be ascertained by reference to the *DoubleClick* case,[39] which came up as a result of an investigation by the Federal Trading Commission (FTC), into allegations made by privacy advocates that DoubleClick, Inc. was indulging in restrictive and unfair trade practices within the meaning of the FTC Act of the United States:

> *[The] DoubleClick server identifies the user's profile by the cookie identification number and runs a complex set of algorithms based, in part, on the user profile, to determine which advertisements it*

---

[35] *Electronic Transactions Act No 19 of 2006*.

[36] C Reed and J Angel, *Computer Law* (Oxford: OUP, 2007), 332.

[37] A person who gains access to computers without permission.

[38] See http://www.microsoft.com/security/glossary.mspx.

[39] *In re Doubleclick Inc. Privacy Litig.*, 154 F.Supp.2d 497 (S.D.N.Y. 2001).

> *will present to the user. ... Meanwhile it also updates the user profile.*

Thus, websites can often record information of the user's preferences and adapt accordingly to suit the user. This is in a way convenient to users, but may become a menace if the websites trigger pop-up advertisements, which is an annoying experience for most users. Also, this may become a hazard to privacy as the gathered information relates to the user's choices and preferences.

Of course, cookies can be disabled in Internet Explorer and Netscape Navigator.[40] Yet websites that require cookies would not be accessible to the user in that case. Thus, as said before, "cookies" – at least in the *online* world are most certainly not as delicious as the cookies that are manufactured by our favourite confectioner. Cookies must not be misused and the usage of it for commercial advertising purposes must be strictly regulated.

8.2.2. The Web Bug: Not the Spider

The Web Bug, is another mode in which user movements on the internet can be monitored. The methodology is to use images known as GIFs[41] in the webpage to trace the movements of the Mouse and Cursors. Also, if sent with email, this can be used to determine if the email has been read by the recipient and if it was forwarded, and to whom it was forwarded. This can be a clear peep into one's individual privacy. A case that is illustrative of the damage that can be caused by the use of Web Bugs was the privacy litigation concerning *Pharmatrak, Inc*.[42]

There, the plaintiffs (internet users of pharmaceutical websites), brought a class action against a number of large pharmaceutical companies that operated websites, and against the data mining and profiling company, Pharmatrak, Inc. The latter company was hired by the pharmaceutical companies to monitor their websites and to provide a monthly summary of website traffic. As part of the agreement with the companies, Pharmatrak represented that it did not collect "personally identifiable information". However, the plaintiffs alleged that a separate contract between Pharmatrak, Inc. and the pharmaceutical companies to install particular software that used a type of technology which could generate personally identifiable data was violating the Electronic Communications Privacy Act of USA. However, Tauro J dismissed the case, adopting the narrow view as in the *Doubleclick* case[43] that information so gathered was not used for a criminal or tortuous purpose. Though the court in this case dismissed the application, it is nevertheless illustrative of the danger that Web Bugs can pose to internet users.

---

[40] Commonly used internet browsing software.

[41] GIF, which stands for 'graphics interface format', is a de facto standard for graphic images on the web. The term 'web bug' was coined by Richard M Smith to refer to GIF files used to monitor internet use. Richard Smith's web bug FAQ is available at http://www.privacyfoundation.org/.

[42] US District Court, District of Massachusetts,Civil Action No 00-11672-JLT, 13 Aug 2002.

[43] See note 39.

8.2.3. Net Spies

Certain pieces of software can be programmed to collect information about the user without his consent and, in most instances, without him even knowing. These pieces of software are known as Spyware. This form of privacy attack can be regarded as more modern than its counterparts, and more damaging to computer users.

Paul Schwartz (in his article titled "Property, Privacy and Personal Data")[44] states that, "Spyware is a program that installs itself without your permission, runs without your permission, and uses your computer without your permission." He concludes by stating that "Data gathered by spyware, are a commodity likely to be sold time and again among third parties such as manufacturers, retailers and market research firms."

8.2.4. Botnets

A Botnet (short for "robot network") is a network of zombie computers,[45] possibly consisting of tens or thousands of zombie computers, which can automatically send out spam messages. From a single computer, a botnet can send thousands of spam messages in one day. Computer systems in Estonia were attacked by Botnets causing electronic havoc in the form of "denial of service attacks".[46] The primary threat from botnets comes from "criminal groups, which try to get personal information to steal someone's bank account"[47] and to perform other forms of organised privacy invasion.

8.2.5. Phishing

In the field of computer security, phishing is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication. Communications purporting to be from popular social web sites (Youtube, Facebook, Myspace), auction sites (eBay), online banks (Wells Fargo, Bank of America, Chase), online payment processors (PayPal), or IT Administrators (Yahoo, Internet Service Providers, corporate) are commonly used to lure unsuspecting computer users. Phishing is typically carried out by e-mail or instant messaging, and it often directs users to enter details at a fake website whose Uniform Resource Locator (URL), look and feel are almost identical to the legitimate one. Even when using Secure Socket Layer[48] with strong cryptography for server authentication, it is practically impossible to detect that the website is fake. Phishing is an example of social engineering techniques used to fool users, and exploits the poor usability of current web security technologies.[49]

---

[44] P Schwartz, "Property, Privacy, and Personal Data" (2004) 117 *Harvard Law Review*, 2056.

[45] Computers infected with a "Backdoor Trojan" that listens for remote commands and carries out remotely controlled actions.

[46] A Denial of Service Attack involves launching huge volumes of e-mail or other messages (more than the target system can handle) from multiple locations, thus disabling the target.

[47] Available at http://preview.tinyurl.com/5bw52o

[48] Secure Socket Layer is an encryption technology on the server that scrambles important data such as credit card numbers and order information when it is being stored or passed from one computer to another. Available at http://en.wikipedia.org/wiki/Transport_Layer_Security

[49] Available at http://en.wikipedia.org/wiki/Phishing#cite_ref-0

8.2.6. Social Networking

Humans are social creatures. Over the years, IT has embraced almost every aspect of human life and has not failed to take into account the sociable quality of people. The social habits and behaviour of humans have been given an electronic facelift by the IT industry, giving rise to the concept of "social networking".[50] However, the large volume of personal information that is fed into these Social Networking Sites (SNSs) by computer users poses a serious threat to individual privacy. Thus, SNSs are an information heaven for potential computer criminals who prey on personal information found on the internet.

8.3. Cable Television: Who is Watching Whom?

Recent developments in the cable television industry are vivid examples of how privacy invasion may occur in one's own household. The latest technology that is used in data transmission through satellites involves a two way process, where data can be both sent and received by the service providers.

As W Lutz, a licensed law enforcement planner in the Department of Administration and Finance, Camden, New Jersey, USA notes:

> *What is disturbing about this development is the ability of cable companies to conduct real-time monitoring of viewer preference in TV entertainment and information access, offering simultaneous send/receive signals while the viewers are watching their shows. A detailed record of what, when and how long a viewer watched any particular show at any given moment is enhanced through new cable television technology. If the average consumer was aware of this fact prior to purchase, would he readily accept the offer?*[51]

It must be noted that the Sri Lanka Rupavahini Corporations Act[52] (which regulates the broadcasting of television programmes) would also cover cable television transmission. Perhaps these can be empowered by the relevant Minister to ensure that malpractices such as those discussed by Lutz are not committed by cable television companies in Sri Lanka.

9. Technology Developments v. Law in Sri Lanka

The Sri Lankan legal regime does not provide for the legal recognition of the right to privacy in any general sense, except in some limited situations which are not far reaching enough to cover modern trends in technology. Apart from the *actio injuriarum* (which seeks to protect damage to feelings), it may be noted that "copyright is capable of helping to resist invasion of privacy".[53] In *Ashdown v*

---

[50] M Marsoof, "Social Networking and its Privacy Implications" (2008) 1 *The Junior Lawyer*, 27.

[51] Available at http://www.asis.org/Bulletin/Feb-97/Lutz.html.

[52] *Sri Lanka Rupavahini Corporation Act No 6 of 1982*.

[53] W Cornish and D Llewelyn, *Intellectual Property: Patents, Copyright, Trade Marks and Allied Rights*, 5th ed., Sweet & Maxwell (2005), 302.

Telegraph Group Ltd.,[54] the English Court of Appeal recognised the right to privacy under copyright law, disapproving of submissions made on behalf of a newspaper on the basis of its freedom of expression. Furthermore, the moral rights attached to one's literary work play a significant role in giving protection to the privacy aspects of such moral rights.[55] These are the limited situations in the realm of private law where privacy is protected.

The dearth of effective laws for the protection of privacy in the field of private law has broad implications that need to be addressed in supporting the contention that the right to privacy warrants protection under public law. Sri Lanka has already adapted to new technology. The step taken by the policy makers to enact the Information Communication Technology Act[56] clearly establishes the intention of the Government of Sri Lanka to convert Sri Lanka into an *e-literate* nation. As a consequence, several new programmes have been initiated by the Information and Communication Technology Agency (ICTA). These maintain a focus on the goal of e-governance. It is therefore necessary to give Constitutional protection to the right to privacy.

9.1. E-Governance

According to the new action plan, the ICTA has proposed the automation of government services and departments. This would be extremely advantageous in the light of public convenience, yet may entail grave ramifications concerning privacy. This form of technology would be a catalyst in creating electronic public records easily accessible by the public.

As Daniel Solove points out:

> *Increasingly as more personal information is collected, stored and consolidated in government databases, the threat to privacy becomes more paramount ... there are a growing number of large corporations that assemble dossiers on practically every individual by combining information in* public records *with information collected in the private sector such as one's purchases, spending habits, web surfing activity and credit history. Increasingly, this dossier of fortified public record information is* sold *back to government agencies for use in investigation people.*[57]

Electronic public records have contributed to the tainting of individual privacy in many countries of the globe, and if Sri Lanka follows suit, the tendency for misuse of public records would spread like a plague.

---

[54] *Ashdown v Telegraph Group Ltd.*, [2002] Ch. 149.

[55] See Sections 9, 10 and 22 of the *Intellectual Property Act No 36 of 2003*.

[56] *Information Communication Technology Act No 27 of 2003*.

[57] D Solove, "Access and Aggregation: Public Records, Privacy and the Constitution" (2002) 86 *Minnesota Law Review*, 1137.

9.2. Electronic Vote

In a democratic society, franchise plays an important role. Perhaps the e-governance formula of the ICTA may lead to electronic voting. This could pave the way for a higher percentage of votes being cast without the voters having to waste precious time travelling to polling stations. However, as efficacious as it sounds, this too may lead to serious erosions to preserving confidential information.

The right to vote was recognised as an extension of the freedom of expression guaranteed in terms of Article 14(1)(a) of the 1978 Constitution in the seminal judgment of Justice Mark Fernando in *Mediwaka v Dayananda Dissanayake.*[58] His Lordship observed that:

> *The citizen's right to vote includes the right to freely choose his representatives, through a genuine election which guarantees the free expression of the will of the electors: not just his own. Therefore not only is a citizen entitled himself to vote at a free, equal and* secret poll*, but he also has a right to a genuine election guaranteeing the free expression of the will of the entire electorate to which he belongs.*

Thus it goes without saying that a person's freedom to vote encompasses his right to choose his representatives in total secrecy. Any electronic voting system must be secure enough to ensure a secret ballot and all necessary precautions must be taken to prevent a breach of confidentiality.

Franchise reflects the political opinion and inclinations of citizens. These ought to be considered as exclusively private. Therefore, the mechanism by which such views are expressed – the electronic voting process – should respect the privacy of individual choice. Therefore, if an electronic voting system is implemented as part of the e-governance programme, it is imperative that proper safeguards and laws are enacted to ensure that individual privacy is guarded, especially against unwarranted executive and administrative action.

9.3. Electronic Commerce

E-Commerce has taken the commercial world by storm and the trend is rapidly changing how business is conducted all over the world and in Sri Lanka too. In Sri Lanka, the Electronic Transactions Act[59] has been the impetus for the creation of an appropriate atmosphere for the encouragement of electronic transactions. For instance, Section 2 of the Act enacts that the objectives of the Act shall be:

> (*a*) to facilitate domestic and international electronic commerce by eliminating legal barriers and establishing legal certainty;
>
> (*b*) to encourage the use of reliable forms of electronic commerce;

---

[58] *Mediwaka v Dayananda Dissanayake*, [2001] 1 SLR 177.

[59] *Electronic Transactions Act No 19 of 2006*.

> (*c*) to facilitate electronic filing of documents with Government and to promote efficient delivery of Government services by means of reliable forms of electronic communications; and
>
> (*d*) to promote public confidence in the authenticity, integrity and reliability of data messages and electronic communications.

Through e-governance, individuals and private business enterprises will be able to transact business with the government electronically. This could, in turn, increase government control of the private sector, perhaps resulting in the instilling of norms of fair competition amongst business enterprises.

Unfortunately, however, the legislation enacted in Sri Lank does not deal with privacy issues arising from the recent developments in ICT. The only exception to this is the Telecommunications Act of 1996, which provides minimum safeguards in regard to private telephone conversations.

10. Legal Reforms

While Sri Lanka has embraced the silicon era at full throttle, and the policy makers in Sri Lanka are busy focussing on ways and means of facilitating electronic transactions, it is only a matter of time before the need for laws regulating the use of the electronic media would be acutely felt.

When formulating legislation in Sri Lanka for the protection of the right of privacy, it will be important to look into legal principles that have been developed by the courts and legislatures in jurisdictions such as the United Kingdom, the United States of America and India. The idea is not to follow foreign laws blindly, but to consider how much Sri Lanka can borrow from these jurisdictions in evolving the law whilst taking the special needs of Sri Lankan society into consideration.

10.1. Why a Fundamental Right to Privacy?

From this discussion, it becomes apparent that privacy is an important right and that, with the increasing use of technology in Sri Lanka, people are more vulnerable to it being breached. Especially in the light of e-governance, the actions of the executive and administrative authorities need to be monitored and checked in order to ensure that they are not abusing their authority.

In Chapter III of the Sri Lankan Constitution, the Fundamental Rights of the people of Sri Lanka are exhaustively guaranteed. On the surface, it seems that Chapter III guarantees no right to privacy. Article 17 read with Article 126(1) of the Constitution makes it clear that an application may be made to the Supreme Court in relation to the infringement of an individual's fundamental right by executive or administrative action. It has been stated that "A public value of privacy derives not only from its protection of the individual as an individual but also from its usefulness as a restraint on government or on the use of power."[60]

Thus, if the government of Sri Lanka becomes electronically active, and if the executive and administrative arms of government by their actions infringe the right to

---

[60] D Solove, M Rotenberg & P Schwartz, *Information Privacy Law* (2nd ed., Aspen), 61.

privacy of a citizen, such action can be questioned by invoking the exclusive jurisdiction of the Supreme Court only if a right to privacy exists as a fundamental right and not otherwise. It is quite ironic to note that the recently enacted Computer Crimes Act of 2007 (CCA)[61] of Sri Lanka (which is geared towards protecting the right to privacy of Sri Lankans through penal sanction) creates a potential privacy threat. Section 18 of the CCA 2007 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. Of course, 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, in any event, no warrant is required in a case of urgency),[62] this gives rise to a serious dilemma in implementing the CCA 2007. The situation is worsened due to the lack of an express guarantee of a fundamental right to privacy. Furthermore, there are countless instances where peoples' rights have been denied and the excuse of "national security" or "public order" has been forwarded to exclude liability for the culprits. However, if the right to privacy was a fundamental right, unless such a plea comes within the strict purview of Article 15(7) (which spells out the limited instances in which fundamental rights can be disregarded – which have always been restrictively interpreted by courts), the Supreme Court would be reluctant to withhold the relief prayed for by a person complaining of infringement. What must be emphasised is that all this is possible only if privacy is to be regarded as a fundamental right.

10.2. Is there a Fundamental Right to Privacy?

Article 14(1)(a) of the Constitution guarantees to every citizen the "freedom of speech, expression including publication". That is the right to communicate their ideas and experiences to others.[63] Can it also be said that this right includes the right not to express? Can silence also be regarded as a form of expression? If that were the case, it would mean that the right to express includes the right not to express. Also, would it include the right to selectively express to a particular person or a group of persons?

A close analysis of "rights" as developed from time immemorial by jurists, unfolds the theory that all rights have a corresponding duty.[64] Further, "the theory identifies the right bearer by virtue of the power that he/she has over the duty in question. He/She can waive it, extinguish it, enforce it or leave it un-enforced".[65] This decision is a choice exercisable by the right holder. Individual discretion is the single most distinctive feature of the concept of "rights".[66] Several approaches may be suggested

---

[61] *Computer Crimes Act No 24 of 2007* (CCA 2007).

[62] Section 18(2)(a) of the *Computer Crimes Act No 24 of 2007*. The question is who decides whether there was urgency at the time of the interception of the information or communication. If this is to be done by a Court of law *after* the event, the damage to privacy has already been accomplished, and no amount of compensation could redress the grievance of the affected person.

[63] J Wickramaratne, *Fundamental Rights in Sri Lanka*, (Stamford Lake, 2006), 603.

[64] M Freeman, *Introduction to Jurisprudence*, (7th ed., Sweet & Maxwell), 355.

[65] J Mill, *Liberty* (1859).

[66] R Flathman, *The Practice of Rights* (1976).

in supporting the view that a fundamental right to privacy exists *hidden* in Chapter III of our Constitution.

10.2.1. First Approach: Privacy as Expression

As stated earlier,[67] privacy contemplates four aspects. These are, on the one hand, information, communication and bodily privacy and, on the other, territorial privacy. The reason for categorising bodily privacy with information and communication privacy is that body language is part and parcel of communication. It may be argued that the way one dresses, moves his body and the like may be a source of information. Thus, the first three aspects of privacy form part of privacy relating to "communication" in general.

For example, if A communicates with B, A intends only to pass information to B. C who is a third party has no access to the information. If C gains access without A's permission, that would be breaching A's privacy. Similarly, it would breach A's right to free expression, as he only *intended* to communicate with B and *not* C. Therefore if privacy is looked upon from a different angle (that is to say from the point of view of expression), one can build on the argument that freedom of speech and expression clothes the right to privacy.

In the online world, for example, certain websites require permission to be accessed. If an internet user gains access to such a website without permission, then it can be argued that the website owner's right to privacy has been infringed and that (as in the illustration concerning A, B and C above) if one attributes the website owner to be A, the users having proper passwords to access as B, and C the hacker,[68], then, C would have also breached A's right of expression which can be enforced as a fundamental right.

10.2.2. Second Approach: Privacy as Movement

The fourth aspect of privacy is territorial privacy. The right to *free* movement within one's residence and workplace or in public are examples, and if there are limits imposed on movement within these spaces, that would impede on territorial privacy. It must be kept in mind that Article 14(1)(h) guarantees the citizens "freedom of movement and of choosing his residence within Sri Lanka".

The focal point of this right is "freedom of movement". The importance of freedom of movement has been highlighted in numerous judicial decisions in many jurisdictions of the globe. It may be of great value to quote the words of Justice Douglas in *Apthekar v Secretary of State*[69] which are as follows:

> *The freedom of movement is the very essence of a free society, setting us apart. Like the right to assembly and the right to association, it often makes all other rights meaningful – knowing, studying, arguing, explaining, conversation, observation and even thinking. Once the right to travel is curtailed, all other rights suffer just as when curfew or home detention is placed on a person.*

---

[67] See note 31.

[68] A person who gains access to another person's computer or network without permission.

[69] *Apthekar v Secretary of State*, (1964) 378 U.S. 500, at page 657.

While the significance of "freedom of movement" was emphasised in this fashion, Justice Subba Rao in the case of *Kharak Singh*[70] remarked as follows;

> *Where he can do whatever he likes, speak to whomsoever he wants, meet people of his choice without any apprehension, subject of course to law of social control… …If a man is shadowed, his movement is constricted, He can move physically, but it can only be a movement of an* automotion*.*

Therefore, an argument can be put forward that, if one's freedom of movement is restricted by using other means (such as surveillance cameras and the like) and causes some inhibition to exercise one's freedom of movement, that too would amount to a violation of the right of free movement. Thus, if this argument is of any avail, the right to privacy can be uncovered from the right to freedom of movement. In fact, this argument has been upheld by Justice Mathew in *Govindh v Madhya Pradesh.*[71]

If a parallel is drawn with the online world, it may be said that the internet user's right to free movement in that context is to *surf*[72] – freely and without fear – the various websites the internet has to offer. Thus, the use of spyware, web bugs and cookies would impede free movement on the internet and thereby interfere with territorial privacy.

10.2.3. Third Approach: Privacy as an Aspect of Quality of Life

Any law requires to be construed in a manner that renders it workable; this is the essence of the purposive theory of statutory construction. The Privy Council, through Lord Diplock, came to the following conclusion with regard to the placing of fundamental rights in a Constitution: "A Constitution and in particular the part of it which protects and entrenches the fundamental rights and freedoms to which all persons in the State are to be entitled, is given a generous and purposive construction."[73]

While the Constitution of Sri Lanka, in which there is no express mention of a right to life, was interpreted in *Shriyani Silva v Iddamalgoda, Officer in Charge of Police Station, Payagala*[74] and *Wewalage Rani Fernando and others v Officer in Charge, Minor Offences, Seeduwa Police Station and others*[75] to imply a right to life, the Indian High Court of Kerala in *F.K Hussain v Union of India*[76] has pointed out that the right to life is "much more than the right to animal existence, and its attributes are manifold, as life itself". The right to life has to be interpreted in the same spirit as the right to live a quality life and must be capable of being exercised freely, fearlessly and

---

[70] See note 12.

[71] *Govindh v Madhya Pradesh*, AIR 1975 (SC) 1378. See- S Sharvananda S (Justice), *Fundamental Rights in Sri Lanka*, 385.

[72] Means to "access" in internet terminology.

[73] *Attorney General of The Gambia v Jobe*, [1985] L.R.C (Const.) 556.

[74] *Shriyani Silva v Iddamalgoda, Officer in Charge of Police Station, Payagala*, [2003] 2 SLR 63.

[75] *Wewalage Rani Fernando and others v Officer in Charge, Minor Offences, Seeduwa Police Station and others*, SC (FR) Application No 700/2002.

[76] *F.K Hussain v Union of India*, AIR 1990 (Kerala) 321.

with affordable privacy. A lack of protection for the right of privacy would undoubtedly impede on the quality of a person's life.

Fundamental rights ought to be construed in the light of directive principles of State policy. This is no novel argument and has been recognised in several important cases in Sri Lanka.[77] Thus, the Constitution, in directing the State to establish a democratic society in which the fundamental rights and freedoms of People will be fully realised;[78] an adequate standard of life would be attained by the People;[79] the moral and cultural standards of the People would be met;[80] human personality would be fully developed;[81] the democratic structure of government and the democratic rights of the people would be broadened and strengthened;[82] social security would be ensured;[83] the family unit would be recognised and protected;[84] and the interests of children and youth would be promoted to ensure their full development[85] places emphasis on the quality of life of an individual. Such emphasis on the quality of life would be of no avail if one were to disregard privacy.

It is highly improbable that the legislators of Sri Lanka deliberately omitted to include privacy as a fundamental right. Perhaps no legislator can be expected to envisage all contingencies and to formulate legislation to cover all situations that might possibly arise. It is for this reason that courts ought to interpret law in a manner that upholds the fundamental rights of the people. In fact, Article 4 of the Constitution affirms this position by compelling all arms of government (including the judiciary) to protect and respect the fundamental rights of the people.

Therefore, it may be urged that the courts have to see through the printed words of the Fundamental Rights Chapter of the Constitution and infer a fundamental right to privacy which is imperative to the citizen – especially in the light of the digital revolution.

11. Conclusions

This paper discusses the importance of privacy as an individual right and the ways in which privacy can be impinged upon in the electronic world. Whether or not courts recognise privacy as a fundamental right under the existing Constitution, the time has come for law makers to consider the inclusion of an express provision in the Constitution establishing a fundamental right to privacy. The importance and necessity to recognise privacy as a fundamental right cannot be understated.

---

[77] *Seneviratne and another v University Grants Commission*, [1978-79-80] 1 SLR 182, *Athukorale v Attorney General*, [1996] 1 SLR 238, *Bulankulama v Ministry of Industrial Development*, [2000] 3 SLR 243.

[78] Article 27(2)(a).

[79] Article 27(2)(c).

[80] Article 27(2)(g).

[81] Article 27(2)(g).

[82] Article 27(4).

[83] Article 27(9).

[84] Article 27(12).

[85] Article 27(13).

However, this does not mean that granting of a constitutional backing to privacy would conclude this debate. Sri Lanka needs a set of comprehensive laws that stems from this constitutional right, to cover various situations that could arise in the future. The delays inherent in Sri Lanka law do more than frustrate litigants. They are a prime reason why a basic and fundamental right such as privacy requires to be recognised as a fundamental right so that aggrieved persons may obtain expeditious relief by invoking the jurisdiction of the Supreme Court.

Furthermore, tribunals and commissions must be established to regulate and maintain standards in electronic transactions and to act as watchdogs to ensure that the government (or any other private entity) keep within the bounds of their authority and do not encroach on the privacy of people.

The primary object of this paper is to highlight the changes in law that are required in the law to ensure the protection of the privacy of Sri Lankans who live in an *information society*. It must be emphasised that this paper is not intended to be conclusive and there are numerous factors to be taken into account in reforming the Sri Lankan law relating to privacy and data protection. The law makers must consider not only the law as it stands, but also the developments in technology, social values, competing interests and contingencies that need to be regulated by law in bringing about a more effective legal framework to protect privacy rights. It has been rightly noted that:

> *While instructive and illuminative, law cannot be the exclusive material for constructing a concept of privacy. Law is a product of the weighing of competing values, and it sometimes embodies difficult trade-offs. In order to determine what the law should protect, we cannot merely look to what the law* does *protect.*[86]

For proper human existence it is neither practical nor possible for there to be absolute privacy as humans are creatures who survive on communication. Every single human act directly or indirectly affects those who are closely connected to him and, to a certain degree, society at large. If such an act violates any law, and causes harm to any person, he can seek redress from a court of law. If such conduct does not violate any specific duty to the public or any law – or does not cause perceptible hurt to any individual except himself – there is nothing society can do and will have to bear the inconvenience.

In conclusion, privacy, though not an absolute right, must not be treated as immaterial. The right balance must be found and the right to one's privacy should always be respected. Whenever the right to privacy is taken away or restricted, it must be done so for valid and good reasons and not otherwise. In developing economies such as Sri Lanka, everything rests on trade, and business in the twenty-first century places much reliance on electronic communication. In fact, very soon we will use electronic tools for governance. Therefore, having laws facilitating electronic transactions will only be beneficial if those who use the new technology can do so with confidence. Information privacy is of great importance for building confidence amongst traders, consumers and the public. Privacy indeed is a right that is to be treasured.

---

[86] D Solove, M Rotenberg and P Schwartz, *Information Privacy Law* (2nd ed., Aspen), 39.