DOES THE INFORMATION AGE CALL FOR *SUI GENERIS* PROTECTION?

Gayathri Liyanage

Attorney-at-Law,
LL.B (Hons)(University of London)

The advent of the electronic computers transformed the economy of the industrial revolution to a digital revolution. Almost overnight the world witnessed the economy being characterized by valuable intangibles as opposed to mechanized tangibles.

The digital revolution ushered in the information age. The information age is characterized by information technology. Information Technology or IT as it is famously acronymized, is the use of computers to store, retrieve, transmit and manipulate data. Different civilization of the world for time in memorial have adopted many mechanisms of organizing data, yet for all the information age digitalized data organization. This was complimented with techniques of processing, the application of statistical and mathematical method to decision making and simulation of higher order thinking through computer programs. As a result, the world as we knew it before birthed a virtual and ubiquitous parallel version of itself.

In this parallel version of the world, individuals are digitally present. Each individual's bio data, financial data and even behavioral patterns are monitored and records of the same are stored in some place in some city in some country that is not known to such individuals. Let along storing this data, data can be accessed and retrieved from data 'warehouses' by persons or even robots with or without the owners' consent. The environment of this virtual and omnipresent world raises two important concerns. Firstly, it challenges the personal space and privacy of an individual. Secondly, it raises the concern as to whether property rights of the information age remain adequately secured.

This articles studies whether the protection afforded by the prevailing laws provides sufficient protection for the two concerns as raised above. Part I will discuss the challenges privacy is faced by the further evolving information age. Part II will focus on whether the prevailing intellectual property law provides protection to the intangible property of the digital revolution, specifically Computer Software.

PART I

***SUI GENERIS* PROTECTION FOR INFORMATION AND INFORMATION SYSTEMS**

'All human beings have three lives: public, private and secret.' –Gabriel Garcia Marquez

The right to privacy is recognized as a human right. International law in general proscribes the interference to privacy and terms the same as unlawful.[1]To the extent that it recognizes that even children and young people have a right to privacy. [2] Regional bodies such as the European Union protects the right to privacy of human beings.[3] This right essentially recognizes "privacy" is inherent to all human being. The expectation of privacy is to protect the dignity of human being. Contextually the dignity of a human being includes such person's self-worth and self-respect. Accordingly privacy affords a person a sphere within which he or she can behave without the interference by any person or thing. On the other hand privacy affords a person a safe heaven from being subject to arbitrary and unjustified use of power by reducing the contents known of a person.

Prior to the virtual world enabled by the digital revolution the sphere of privacy was adequately protected. That is, only information that was disclosed was considered to be publicly available and where information disclosed was to be confidential, laws on non-disclosure and confidentiality would sufficiently apply. In order to study whether modern information or data can even be treated in this similar classification one must understand the nature of information in this information age.

Information unlike before is digitalized and is ubiquitous. Digitalized information is expressed as a series of 1 and 0 and computed as per a binary system. Therefore inherent to all digitalized information is its ability for large volumes of information to be stored in different binary computations and its ability to be transmitted rapidly, stored and even copied or duplicated without a hassle. Hence rendering information vulnerable in this day and age.

Information is 'everywhere' in this information age. It has affected the learning, diagnostics, management, physical planning, finance, entertainment and communication. (Munshi, 2002). Businesses and commerce more or less have transformed into digitalized technology. Consequently large volumes of information are extracted from individuals. Whether it being with online shopping, online accommodation reservation or simply having dinner delivered home individuals share a great deal of information that maybe

[1] Article 12, United Nations Declaration of Human Rights, Article 17 of the International Covenant on Civil and Political Rights

[2] Article 16 Convention on the Rights of the Child

[3] Article 8 European Convention for the Protection of Human Rights and Fundamental Freedoms

used to identify them. Therefore although the box with the terms and conditions is 'checked' to receive the service little are beneficiaries of such services aware of the traces they leave with their online presence and is oblivious to the factor that such information is processed.

One of the largest modern data scandals was when Cambridge Analytica unlawfully accessed the data of 87 million Facebook users and had used such data without consent for a political advertising campaign. Large quantities of data was harvested by Cambridge Analytica by the use of an application called 'thisisyourdigitallife'. Although through API Cambridge Analytica was able to access the information of Facebook users and the Facebook CEO Mark Zuckerberg did take responsibility really speaking the onus remains on the users itself to know and intelligently share information. It was revealed in 2017, that the databases of Uber was hacked and that information of over 57 million customers and drivers had being hacked into in 2016.

The traditional laws on confidentiality and non-disclosure proved to be redundant and sophistically impotent to safeguard the reformed nature of information. As the nature of this information permits it to be rapidly transmitted and retrieved not only by the parties authorized with such information but also by other persons or bodies. Therefore it becomes important in the information age not only to regulate responsible access of this information but also to control the duplication and transmission of this information.

In addition when protecting the confidentiality of information it is not only the information that must be protected but also the infrastructure in which such information is stored. That is information systems must be secured from accidental and intentional misuse by persons. Information systems need to be protected from unauthorized access by third parties such as employees, past employees, foreign states, suppliers and even hackers. Furthermore, these systems need to be safeguarded from malicious software such as malware, Trojan horses, SQL injection, spyware.

In a generic sense the world does enjoy some protection from cybercrimes. Fraud is a general term used to describe a cybercrime that intends to deceive a person in order to gain important data or information. Fraud can be done by altering, destroying, stealing, or suppressing any information to secure unlawful or unfair gain. However, the legal infrastructure is yet to directly secure users from cyber probes such as spamming, cyber stalking, Phishing, social engineering and mal-advertising.

When it comes to phishing, phishers use "email spoofing" to extract confidential information such as credit card numbers, social security numbers and passwords. The users receive emails carrying links to bogus websites. Users believing that these websites

are legitimate will enter personal information.

Social engineering is a method in which cybercriminals make a direct contact with individuals and obtain important information from such individuals.

Malvertising is the method of filling websites with advertisements carrying malicious codes. Once this is clicked the user will be redirected to a fake website or a file carrying viruses and malware will automatically be downloaded.

Cyberstalking involves following a person online anonymously. The stalker will virtually follow the victim, including his or her activities. Most of the victims of cyberstalking are women and children being followed by men and pedophiles.

From the exiting legal regimes it can be determined that the protection provided is merely an extension or a re-shaping of the traditional principles of protection. The use of computers to commit a crime is correctly a computer crime for which adequate laws are available. Fraud is as commonly understood the application of deceit for person or some other gain. However, the author is of the view that such law do not address the core vulnerabilities created in information age. Therefore the principle of protection do not articulate to the concepts of the information age. For an example legal infrastructure can be further developed regulate the use of IP addresses that maybe used for spoofing, distribution of malicious codes. Further, the author is of the view that the prevailing legal regimes does not address the very fact of a virtual platform and a digital environment. It is suggested that a sui generis system of laws could recognize offences such as digital misrepresentation and digital trespassing and regulate hacking that is allegedly lawful and not. It is also matter of policy whether such offences are to be treated with criminal liability or not.

However, unlike protection for the it infrastructure the protection for information is being reformed as we speak and the world is transgressing into an advanced form of information protection. Fashionably referred to in the modern day as ‘data protection’. Perhaps the latest revolution of data protection is with the European Union Regulation - General Data Protection Regulation (GDPR).

The GDPR invariably births a new creature of law that recognizes ‘protection of natural persons in relation to the processing of personal data’ as a fundamental right and bestowing on every individual or data subject the ‘right to be forgotten’. The lacuna of the previous protective regimes perhaps is recognizably the inability to regulate the ‘processing’ of data which, the GDPR in all its might attempts to secure. The GDPR while attempting to afford the requisite protection to natural persons is designed to respect the processing activities to also ensure a free flow of personal data legitimately.

Any information relating to an identified or identifiable natural person is termed as 'personal data' hence plastering all the shortcoming of 'information' of a person as it was primitively known. While the 'processing' is broadly defined to include any operation or set of operations performed on personal data. Thereby intending to include within its scope any activity that can be performed on such data. The obligation of regularized protection is the responsibility of an identified Controller[4] and Processor[5]. The responsibility is such that personal data is to be Pseudonymized[6] or masked.

In the wake of the GDPR in the pipelines of the Sri Lankan legislative system is a Data Protection Bill at the time of writing this article. The draft Data Protection Bill is inspired by the GDPR and with its enactment will toil to the benefit of all Sri Lankans citizens.

PART II

SUI GENERIS SYSTEM OF PROTECTION OF COMPUTER SOFTWARE

"Since when has the world of computer software design been about what people want? This is a simple question of evolution. The day is quickly coming when every knee will bow down to a silicon fist, and you will all beg your binary gods for mercy."-Bill Gates[7]

With the massive growth of the software industry and also the products generated from it reflect the importance of the same to the world economy. Investors and innovators in this industry require predictable and certain laws for protection. Copyrights and patents have failed to provide such uniform protection. A *sui generis* system for the protection of computer software has been suggested as the solution. The concept of a *sui generis* system of laws for computer software is not a novel concept. It has been proposed in early as the 1970s[8]and throughout at different intervals in time for the past five decades or so, however, quite interesting none of these systems have effected. Amidst the haste for better protection of computer software, such hinder on the development of the system has

[4] Means the natural or legal person, public authority, agency or other body which alone or jointly with others, determines the purposes and means of processing of personal data;

[5] Means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

[6] Means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information.

[7] William Henry Bill Gates III (October 1955) is an American business magnate, philanthropist, investor, computer programmer, and inventor. He is the former CEO and Chairman of Microsoft. (http://www.brainyquote.com/quotes/authors/b/bill_gates_2.html retrieved on 06.05.2014)

[8] US *sui generis* software protection, which failed due to technical flaws as was contested by the Antitrust Division.

been rather strange. The reason that no *sui generis* system has progressed to date maybe because although there is much anticipation for this brand new system no body or organization has settled on the policies or the direction that should take by such a system. This is also demonstrated in the different systems of *sui generis* law proposed by different organization. The WIPO Model Provisions take a more copyright approach in steering protection while the Computer Software Protection Act proposed by Commissioner Hersey of CONTU is guided by a hybrid of laws between copyrights and patents.

Although the WIPO model provided a well drafted system of protection for computer software. It is criticized because it does not provide for ownership of rights of computer output and also does not create incentives to drift from non-disclosure contracts with third parties. *Prima facie* Commissioner Hersey's proposed model seemed to be promising as it guaranteed the best of both worlds. Under this approach both the expression and innovative ideas involved in the creation of computer programs would be granted protection. Unlike in the WIPO Model Provisions this Computer Software Protection Act provided for Registry of Computer software. The problem with such a registration system will be to identify the classes that particular type of software can be categorized as and also how the categories will be identified when the software is upgraded. Also a mandatory system of registration has other disadvantages. That is sometimes full disclosure is unrealistic until proprietors can be assured that they will be fully compensated for any violations of their rights in the product.

Under the Computer Software Protection Act the subject matter that receives protection will include the product of original intellectual effort, produced in any form or medium, and which includes as one of its component elements a computer program. The phrase "in any form or medium" would permit protection for programs embodied in written materials, source code, object code, microde, or any medium of fixation to be developed in the future.

It is interesting to note that both these *sui generis* system of law provides for a distinction between computer software and computer programs. Computer software is defined to include the utility and the function aspect of computer programs as well as the accompanying documentation which includes flowcharts, manuals and other specification.[9] The definition introduced to by the Computer Software Protection Act encircles hybrid nature of

[9]The WIPO Model Provisions defines Computer software to include either Computer Program; Program Description; Supporting Material; or several of these components. The definition extends to protect all types of Computer Programs; and The Computer Software Protection Act broadens the definition of computer software to include computer program and also documentation incidental thereto.

protection and it does not envisage protection of any element in a Computer software which merely incorporates a mathematical relationship or a scientific principle. The scope of protection maybe further supplemented by the concept followed in the Freeman-Walter-Abele Test[10]. That is, the protected subject matter should be claimed with respect to the innovative element and not the building blocks of it like algorithms.

In the 1980s the Japanese Ministry of International Trade and Industry in its report concluded after studying the worrying effects of the expanded copyright law suggested that Japan adopt a *sui generis* form of protection for computer software. However, the progress of there recommendations were halted by the mafia companies that favoured copyright protection.

Although conceptions of a *sui generis* system were withdrawn the society was not without the question of inappropriateness of copyright laws and patent laws. Computer software is a product of both expression and innovation and the intellectual property law is silent on the protection of such a natured product. The difficulty with both these types of protection is that "they do little -and do too much- for software and its non-code aspects."[11]

OPPOSITION TO A *SUI GENERIS* LAW

There is thinking on the line that the call for *sui generis* for software protection is an exaggeration of the lacuna of laws at present. It is stated that although computer software is unique, each aspect of its dual nature can be understood separately in the context of prior technology forms of expression. Therefore, enabling protection using traditional forms of intellectual property law. This perception at different degrees is what we saw in the preceding chapters expanding the usual boundaries of copyright law and patent laws. All laws in this arena attempt to protect the innovative effort included in computer software and such innovation is the result of mental process. Although the subject matter of traditional copyrights and patents are different to computer software, the innovation found in such creation is also the product of a mental process. It is in view of this argument that further debate on opposition to *sui generis* system has triggered. As an alternative patent protection of computer software is proposed.

One of the primary objections for patent protection of Computer software is the fear that the software industry will come to a standstill. The stringent monopolies secured by patent laws propagate adverse concerns.

[10]Arrhythmia Research Technology, Inc v. Corazonix Corp 958 F.2d 1053 (Fed. Cir.1992) speaks of the Freeman-Walter Abele Test

[11] Should We Consider Another Model of Industrial Property Rights in Software? Address by Richard H Stern

In reality no amount of ideas can be said to saturate the software industry.[12]

Computer software is indeed the result of innovation and expression. Theoretically, they can be protected separately in terms of patents and copyrights. However, the demand is not for such a solution. It is identified that such protection is "short sighted [solution] to complex problems."[13] As stated in Altai trying to fit in protection of computer software into tradition intellectual property laws is like trying to fit a square peg into a round hole. To create certainty and predictability of protection the software product as a whole must be able to secure protection.

The basis of any system of law for the protection must rest on the common interest and goals of policymakers. Hence it is commonly recognized that it has to be a system of law that encourage technological progress, spread of knowledge, industrial efficiency and free competition. These interests are met by encouraging disclosure of information and in turn for securing an economic benefit to the creator or author. It is in securing this interest and striking a balance that policy makers more often than not get stalled. Disclosure is a clean goal to set however, it is not viable in the sense of computer software because it is vulnerable to counterfeit products and piracy.

Although computer software is now the problem, jurisprudence of many laws tells a similar story, example the semi-conductor industry[14]. In this respect the US policy makers adopted a. A system of petty patents and utility model has been considered for computer software protection. The latter on the basis of copyright regime.

SUI GENERIS PROTECTION OF COMPUTER SOFTWARE

The most favoured type of protection for computer software will be a hybrid type of laws as professed by Commissioner Hersey. Then legislators are enriched with the jurisprudence of copyrights and patents as the base understanding of this system. This *sui generis* system of protection for computer software will lay out a comprehensive definition of computer program in the drafting of a new set of law in terms of *sui generis* system of protection it will be helpful to have the sum of the definitions already provided in the WIPO Model Provisions and the Computer software Protection Act together with the accession to protection of look and feel.

The protection afforded under this model should protect the expression of the idea

[12] John M. Griem, Jr , Against a Sui Generis System of Intellectual Property for Computer software, in Hofstra Law Review Volume 22 Issue 1 Article 4 argument that the software industry has already seasoned with ideas that there is no longer the need for circulation of ideas on software development is without merit.

[13] Pope & Pope, Protection of Proprietary Interest in Computer software

[14]Semiconductor Chip Act 1984, this based on a utility model system creating a proprietary right for semiconductor chips.

instilled in the computer software. Thence, extending its protection to source code to object code and also the development process and flow charts. The right secured to such original work of authorship must be guarded against infringers adopting "substantially similar" software.

Also this law must serve to protect interfaces and not exclusively protect the structure of computer software. Interfaces should be protected as it is what adds efficiency and attraction to the software, therefore exhibiting vulnerability to be easily misappropriated. However, the structure of computer software must not be monopolized as that will have stationery effects on the software industry. Structure of computer software can be understood to be the primary reason the program is formulated and the basics of navigating in that program. The rights granted to software creators must only be limited to the economic right as moral rights are impractical in the utilitarian nature of computer software. Further, research involved in this paper suggests that the doctrine of fair use should not be coupled into the rights of software creators, as software is immensely vulnerable to being misappropriated and immediately altered in nature. However, in the interests of competition law and education of the public, reverse engineering[15] or decompilation must be allowed to facilitate operability.

Significantly, inspired by the semi-conductor laws, duration of protection of computer software must be ten years sufficing ample time to recoup on investment.

This *sui generis* system must be proposed as an international treaty must be drafted and proposed by a powerful organization like the World Trade Organization for it to have effective strength in its operation[16].In order to allow this new system of laws to be absorbed into national laws in their own yardstick the principle of "minimum rights" can be adopted. Thereby being careful not to stir any unnecessarily incompatibilities, In order to achieve uniformity of laws and equal protection for the industry "national treatment" and the "most-favoured-nation" principle shall be provided.

CONCLUSION

The author is of the view that the dynamics of the world have drastically changed from the industrial revolution. Although many facets of business, industry, commerce and even daily life seem like it's a continuation from the previous era. In reality, the landscaping of all such facets have intrinsically changed. For an example, while it is a fact that we exchange consideration for purchasing of goods. In most cases the

[15] US Supreme Court defined reverse engineering in Kawanee Oil Co. v. Bicron Corp., 416 US 470 (1974) as starting with the known product and working backward to divine the process which aided in its development or manufacture."

[16] Similar to how TRIPS was effected.

exchange of value takes place swiftly via platforms and infrastructure that is itself for is owned and operated by separate mechanisms. In time to come, the features of cryptocurrency and cryptography will secure commercial deals. Even then if the only action that policy makers and legislator can do is to stretch the existing principles and await the adjudicator to exaggerate the same in the name of justice, the citizens of the world are up for being more vulnerable than ever before.