INTERCONNECTION BETWEEN INTELLECTUAL PROPERTY RIGHTS AND CYBER SECURITY

By Ishaan Behal and Ragini Rao
From Amity Law School, Noida and Ansal University, Gurgaon respectively

Abstract
This paper is an attempt to depict Intellectual Property Rights in accordance to cyber space. At present, the legislative framework regulating IPR in cyberspace is inadequate to cope with all the components of cyber security. The existing laws are getting outdated and should be revised in order to adapt to the dynamic nature of the digital world, to maintain the quality of protection and regulation they provide
Some key questions which are answered in this paper are -
1) How are Intellectual Property Rights connected with cyber space ?
2) What kind of Intellectual Property Rights are available in cyber space ?
3) Are there any loopholes in the legal system regulating IPR in cyber space?
This paper is a twofold scenario which initially describes Intellectual Property Rights and cyber security. Later, it talks about the colligation of the both, by explaining how Intellectual Property can be connected with cyber space and what are the various kinds of Intellectual Property Rights available in cyber space. At the end, this paper also provides some suggestions in order to improvise the current legislative regime regulating IPR in cyber space

Introduction

In the world where most of the population finds it convenient to download software, movies, music etc. for free on the internet rather than purchasing the original version, it gets very easy for the hackers to gain access to our private information. After the emergence of Social media, people don't even think twice before opening and sharing links. This lack of after math has led to loss of confidentiality over their personal data. According to WIPO (World Intellectual Property Organization) Intellectual property refers to creations of the mind – inventions, literary and artistic works and symbols, names and images used in commerce. [1]

In the modern time, the world has been facing a great deal of flood in the Cyber Crime with Globalization being the main factor behind it. Cyber Crimes can be in the form of Bullying over social media, Cyber Stalking, Spamming, Torjan Attacks etc.

In the legal framework of our country, till date only the Information Technology Act, 2000 has been enacted in order to regulate cybercrime. However, time has radically changed from where everything started, in like manner the act needs to go through many further changes so as to adjust to the present day situation. To bring down the cybercrime rate, suitable measures need to be taken at both Legislative and Judiciary levels to keep the guilty parties from infringing upon the law.

Intellectual Property Rights

Intellectual property rights are like any other property right. They allow creators, or owners, of patents, trademarks or copyrighted works to benefit from their own

[1] https://www.wipo.int/about-ip/en/

work or investment in a creation. These rights are outlined in Article27 of the Universal Declaration of Human Rights, which provides for the right to benefit from the protection of moral and material interests resulting from authorship of scientific, literary or artistic productions.[2] The importance of IP was for the very first time discussed in the Paris Convention, 1883 for protection of Industrial Property and then later on in the Berne Convention,1886 for the protection of Literary and Artistic Works. Both of these are regulated by WIPO

WIPO (World Intellectual Property Organization). Is an international organization that administers a number of international agreements that deal partly or entirely with the protection of geographical indications (in particular, the Paris Convention and the Lisbon Agreement).[3]

The following are the list of activities covered by the intellectual property rights, laid down by the WIPO –

- Industrial designs
- Inventions possible in human venture
- Trademarks, service marks, designations etc.
- Scientific Inventions
- Literary, artistic, and scientific works
- Unhealthy competition
- Performances of performing artists, phonograms, and broadcasts
- All other rights intellect
- Intellectual property in industrial, scientific, literary, or artistic fields

Intellectual property rights protecting the cyber space are as follows –

- Copyright Law
- Trademark Law
- Patent law

Colligation of the Intellectual Property Rights and Cyber Space will be further discussed in detail in this research paper.

Cyber Security

Security is the foremost urgency in every aspect of our lives. There has been an extensive growth of cyber security in the software industry. These threats have risen up to a whole different level.

We live in a world where our private information is as crucial as it has ever been. With the rising software industries, it has become truly primary to specifically design something with a framework that retains the integrity and confidentiality of the system as a whole. Everything comes at stake once the extirpation of security takes place.

Cyber security is characterized as giving protection to the network, interface and the system as a whole. It protects the entire framework from the malicious and unauthorized access.

Data theft is the forbidden shift or storage of any information that is confidential, personal, or financial in nature, including passwords, software code, or algorithms, proprietary process-oriented information, or technologies. [4]

Some common modes of data theft are- USB drive, portable hard drive, devices using

[2] http://hrlibrary.umn.edu/gencomm/escgencom17.html

[3] www.wipo.int/edocs/pubdocs

[4] www.itgovernance.co.uk/what-is-cybersecurity

memory cards and PDAs, Emails, Printing, Remote sharing, and Malware attacks.

CYBER CRIME

Cybercrime is characterized by the felonious usage of computer and theft. It has been growing ever since such as viruses, spams, breaking into a server or a network, theft of data thereby breaking its confidentiality, stalking someone and using their information to further bully them, fraudulent activity and so on. Unfortunately, it won't just stop here as there is advancement in the technology more or less there has been a drastic increase in cybercrime. (R)

Things highly affecting cyber security

- **Web servers:**

There are attacks on these web applications to take out data or to pass out the nasty code that exists. Attackers often pass out their nasty code through these web servers that they have already hacked. Henceforth we need something big that protects our web servers and web applications to the core. Web servers have now become one of the most convenient platforms for the attackers to steal data.

- **Cloud computing and its services**

Nowadays every small or large scale company is adopting and working with the cloud and utilizing its services. The world is gradually propelling towards the clouds. This newest technology shows even bigger challenge for cyber security Moreover, as the number of web applications available in the cloud increases, there should also be a huge change in the policy controls for web applications and cloud services so that the valuable information is protected. Cloud may provide many facilities but it should also be considered that as the cloud grows care the security is not compromised.

- **Advanced Persistent Threat**

Advanced Persistent Threat, is a completely different kind of a cybercrime. As attackers grow stronger and incorporate ambiguous techniques, network security must develop other security services to detect attacks. Hence one we should improve our security techniques to prevent threats coming in the near future.

- **Mobile Networks**

We can connect to anyone in any part of the world we wish to through these networks. It is undeniable that these mobile networks need a high end security and it is a major concern. Now a days we can observe that firewalls and other security measures have become way more permeable as we are using devices like mobile phones, tablets, PCs, and so on, all of them need extra security apart from those which are being used in the applications. We must always consider the security that could easily beat stake, with these mobile networks. Mobile networks are easily attacked and they are largely open to these cyber-crimes henceforth a lot of care must be taken.

- **IPv6 - New Internet Protocol**

IPv6 - New Internet Protocol is the new internet protocol that is taking over IPv4 which is the older version of it that has been a support for our entire networks and the Internet as a whole. While IPv6 is a whole

new substitute in making more IP addresses available, there are some basic changes to the protocol that should be taken care of in the security policy. It is better to switch to IPv6 as it is more secure and the cybercrime can be much reduced this way.

- **Encryption of the code**

Encryption is characterized as encoding messages or the given data in a way that nobody else can understand or read except for the concerned user. The message or data is encrypted using different algorithms, converting them it into an unreadable cipher text. There is an encryption key that shows how the message is to be converted or say encoded. Encryption helps in protecting data privacy and its integrity. Encryption protects data in transit, like when data is being transferred through networks like, mobile telephones or wireless. So by encrypting the given or sent code we can discover if there is any leakage of data or the relevant information.

SOCIAL MEDIA IN CYBER SECURITY

Organizations and companies should find new ways to secure personal information as the social media and sharing of information has grown up to a whole next level. Social media is a great deal in cyber security and will invite many personal cyber threats. As social media and social networking sites are used by all of us every day and night it has eventually become a major platform for the attackers for hacking and misusing the private information and stealing our most valuable data.

We see that people are rapidly attracted by the schemes of the social media thereby the hackers or attackers utilize them to gather the valuable information and everything that they need. So, we should take very accurate and appropriate measures in coping up with social media so that we can help secure it and prevent all kind of valuable data loss and theft. With giving someone the authority to broadcast delicate data or information, it also gives the same authority to transmit the bad or false information, which could get equally damaging. The quick transmission of this false information via social media comes under the arising risks identified in *Global Risks 2013* report. [5]

A few international cyber-attack examples are as follows-

- **North Korea 'stole $2bn for weapons via cyber-attacks' -**
  North Korea has stolen $2bn (£1.6bn) to fund its weapons programme using cyber-attacks, a leaked United Nations report says. The confidential report says Pyongyang has targeted banks and crypto-currency exchanges to collect cash. Sources confirmed to the BBC that the UN was investigating 35 cyber-attacks. It follows a string of missile launches by North Korea in recent weeks, with the country's leader Kim Jong-un saying the launches were a warning against joint military exercises being carried out by the US and South Korea[6]

British Airways faces record £183m fine for data breach – The incident took place after users of British Airways' website were diverted to a fraudulent site. Through this

[5] www.rapid7.com/fundamentals/types-of-attacks

[6]https://www.bbc.com/news/topics/cp3mvpdp1r2t/cyber-attacks

false site, details of about 500,000 customers were harvested by the attackers, the ICO said.

Information Commissioner Elizabeth Denham said: "People's personal data is just that - personal. When an organization fails to protect it from loss, damage or theft, it is more than an inconvenience. That's why the law is clear - when you are entrusted with personal data, you must look after it. Those that don't will face scrutiny from my office to check they have taken appropriate steps to protect fundamental privacy rights."

The incident was first disclosed on 6 September 2018 and BA had initially said approximately 380,000 transactions were affected, but the stolen data did not include travel or passport details.[7]

CYBER SECURITY TECHNIQUES

The Access control and password security

We all know generating user names and passwords have always been basic ways of securing our valuable information or data. It might be one of the first acts regarding cyber security.

Authentication of the data

The documents and files that we get should always be authenticated even before downloading them it should be seen whether or not it has originated from a trusted and a more reliable source and that they are not at all changed or disturbed in any way. Authenticating documents is done by the anti-virus software which is present there in the device itself. Thus, a solid anti-virus software is also important to secure the devices from malicious codes also known as viruses.

The Malware scanners

It is software which regularly scans all the files and documents which are located in the system for the bad code or harmful viruses. Viruses or worms or Trojan horses are such examples of malicious software which are frequently clubbed together and known as malware.

Firewall

A firewall is basically a software program which helps in identifying hackers, worms, Trojans, viruses, and so on, which try to get our computers infected or attacked. All the texts entering or leaving the internet go through the firewall which is located there, which analyses each text and then blocks those messages which do not fit in the required security criteria

Anti-virus software

Antivirus is a basically a computer program which identifies, rules out, and intervenes to eliminate pernicious software programs, like, viruses and worms. Most antivirus programs constitute of an auto-update feature that calls attention to. It helps enable the program to download profiles of the newly detected. An anti-virus software is a basic requirement for every single system.

[7] https://www.bbc.com/news/business-48905907?intlink_from_url=

Interconnection between IPR and Cybersecurity

The main objective of this article is to enlighten the readers and the creators of cyber content, about the rights available to them, so as to protect their innovation to be used without their prior permission over the internet.

Various Intellectual Property Rights protecting the data, software and contents available in cyber space are as following –

a) **Copyright –** With reference to Section 13 of the Indian Copyright Act, 1957 it can be stated that, copyright shall subsist throughout India in the following classes of works –

(a) Original literary, dramatic, musical and artistic works
(b) Cinematograph films
(c) Sound recording[8]

Copyright is basically a legal device which gives the creator of the given classes of work, the sole right to sell and publish his work. In the meantime, copyright law has been incorporated and implemented to secure the content available on net. It provides protection to authentic work which is presented in substantial manner. In spite of the fact that the present copyright laws do give security to copyright proprietors, but it can't be ignored that they contain few deficiencies with regards to the adequacy of copyright insurance being authorized on the general population. To overcome these hindrances, we require a more grounded and mightier relationship in different wards along with close participation of various global associations. It is therefore the duty of the society to spread awareness about the need of copyright protection in order to control and prevent unauthorized usage of original work.

The Copyright Treaty 1996 and Performances and Phonograms Treaty 1996 are two major legal instruments at global level relating to cyberspace created under the guidance of W.I.P.O. These treaties give the copyright owner the specific rights to distribute, display and communicate to public. However these sole rights given to the proprietor of the copyright are subject to the doctrine of 'Fair Use'

Fair Use

The doctrine of fair use allows in person to copy or use a copyrighted material for limited and transformative purposes such as to criticize, comment or parody a copyrighted work. Fair use can act as a defense against a claim of copyright infringement if your use qualifies fair use, else it will be an illegal infringement

Database

The term database can be defined as compilation of a particular set of data stored in a computer system. This term was for the very first time mentioned in the Information Technology Act, 2000. The Indian Copyright Act 1957 includes and protects Databases as a part of "Literary Works" under Section 13(1). Also, section 43 and section 66 of the IT Act, 2000 provides for penal liabilities against the person who infringes a copyrighted database and entitles

[8] Section 13 , Indian Copyright Act 1957

the owner of a the copyrighted database, which has been violated for compensation up to one crore rupees

Electronic Copyright Management System

The copyright proprietors have an alternative to utilize the technology security measures. E.C.M.S is a legislative framework to ensure against outsiders evading these systems.

Different kinds of technology protection measures are as following –

1. Access control measures - These kinds of measures prevent outsiders from gaining access to the copyrighted contents. For eg. Setting up of passwords, encryption etc.

2. Duplicate control measures – These kinds on measures prevent copyrighted content from being copied by the third parties. For eg. Disabling right click. Installing piracy protector on movie CDs etc.

E.C.M.S empowers the copyright proprietors to follow, track, and oversee and to avoid replicating of their work or recognize unapproved duplicates made from their original work

D.M.C.A (Digital Millennium Copyright Act 1998)

The Digital Millennium Copyright Act (DMCA) is a 1998 United States copyright law that implements two 1996 treaties of the World Intellectual Property Organization (WIPO). It criminalizes production and dissemination of technology, devices, or services intended to circumvent measures that control access to copyrighted works. It also criminalizes the act of circumventing an access control, whether or not there is actual infringement of copyright itself. In addition, the DMCA heightens the penalties for copyright infringement on the Internet.[9]

b) Patent law - A Patent is basically a government license or permit providing a privilege or title for a set period, particularly to the sole holder of the patent to reject others from making, utilizing, or selling a creation. However, according to the section 3(d) of the Patent Act, 1970. "The mere discovery of a new form of a known substance which does not result in the enhancement of the known efficacy of that substance or the mere discovery of any new property or new use for a known substance or of the mere use of a known process, machine or apparatus unless such known process results in a new product or employs at least one new reactant, is not patentable " [10]

In most of the cases, computer software available for purchase are protected by the means of copyright law. However, in certain cases PC implemented creations can be covered under patent protection if they fulfil the requirements of patentability, The invention must be novel and must not fall under any category mentioned in Section 2 of the Patent Act, 1970 . Whether or not the pc implemented creations furnishes a unique technical effect, is the key question which determines whether the creation can enjoy patentability or not.

[9] https://en.wikipedia.org/wiki/Digital_Millennium_Copyright_Act

[10] section 3(d) of the Patent Act, 1970

The US Supreme Court in Parker v. Flook (437 US 584: 57 L Ed 2d 451) also held that "a method for updating alarm limits during catalytic conversion, which is a mathematical formula, is not patentable." In the Indian legal framework, section 3(k) of the Patent Act, 1970 states that a mathematical or business method or computer programe per se or algorithms is not invention for purposes of the Patents Act[11]

An invention which meets the essential requirement of patentability (novelty, resourceful step, business software) can't be excluded from protection only due to the fact that a computer software was used for its operation. Any technical process carried out through the means of a computer hardware or software has no connection with the computer program, cannot be denied patent protection.

In the case Gottschalk v. Benson (409 US 63: 34 L Ed 2d 273) (the Gottschalk case), the US Supreme Court held that a "computer software, involving a method to convert binary coded decimal numerals into pure binary numerals can't be patented because

- The method was so abstract as to cover both known and unknown uses of the binary-coded-decimal to pure binary conversion;
- The end use could vary and could be performed through any existing machinery or future-devised machinery or without any apparatus
- The mathematical formula involved had no substantial practical application except in connection with a digital computer; and
- The result of granting a patent would be to improperly issue a patent for an idea. " [12]

c) Trade Mark - Trademark is defined under Section 2 (zb) of the Trade Marks Act, 1999 as, "trade mark means a mark capable of being represented graphically and which is capable of distinguishing the goods or services of one person from those of others and may include shape of goods, their packaging and combination of colours." A mark can include a device, brand, heading, label, ticket, name, signature, word, letter, numeral, shape of goods, packaging or combination of colours or any such combinations [13]

A Trademark in cyber security is an agreement between a code that confirms the security characteristics of an article and a code that necessitates an item to have certain security characteristics. It is helpful in guaranteeing secure data streaming. In object oriented programming, trademarking is practically equivalent to marking of information that can regularly be executed without cryptography

Suggestions and conclusion

In this paper, I would like to communicate some suggestions which would help us prevent intellectual property infringement in cyber space.

Firstly, an immediate step which should be taken by the respected authorities is to implement a global convention regulating the cyberspace, in order to cope up with the safety measures required to prevent

[11] Parker v. Flook (437 US 584: 57 L Ed 2d 451)

[12] Gottschalk v. Benson (409 US 63: 34 L Ed 2d 273)

[13] Section 2 (zb) of the Trade Marks Act, 1999

Intellectual property right infringement at an international level. Secondly, any person trying to violate this global convention by infringing the intellectual assets of another user should be made liable to the same legislative punishment, which he would have been, had he been violating any other international convention.

At the end, it can be concluded by agreeing to the fact that the present implemented laws protecting the Intellectual Property Rights in cyber space are getting outdated and are not really enough to fight the humungous problem of Intellectual Property violation in cyber space. These laws need to be revised according to the present conditions in order to stay updated. Also, the establishment of a global agency for tracking and monitoring, intellectual property right violation in cyber space is a must to regulate cyber security

*****