East African Scholars Multidisciplinary Bulletin
Abbreviated Key Title: East African Scholars Multidiscip Bull
ISSN: 2617-4413 (Print) | ISSN 2617-717X (Online)
Published By East African Scholars Publisher, Kenya

Volume-3 | Issue-1 | Jan-2020 | DOI: 10.36349/EASJMB.2020.v03i01.01

OPEN ACCESS

Review Article

Law Relating to Cyber Crimes- Comparative Perspective

Jitender K Malik*[1] and Dr. Sanjaya Choudhury[1]

[1]Department of Law, Bhagwant University, Ajmer, Rajasthan, India

Article History
Received: 04.12.2019
Accepted: 11.12.2019
Published: 23.01.2020

Journal homepage:
https://easpublisher.com/easmb

Quick Response Code

Abstract: In 1996, the Council of Europe, together with representatives from Canada, Japan and the United States drafted a preliminary international treaty covering computer crime. There was some rebellion to this though, as the civil libertarian groups did not approve of the provisions in the treaty which required internet service providers to store customer transactions and be able to turn them over on demand. However, work on the treaty proceeded. This led to the International Convention on Cybercrime in Budapest in 2001; which was signed by thirty countries, including Japan, South Africa, Canada and the US. The convention authorizes a global cyber police force to investigate cyber crime. This meant that investigators had the power to track down network communications and to store intercepted data across countries. For this to work, nations must cooperate with each other by sharing gathered information and evidence related to cyber crime. Additional protocols covering terrorist activities and racist and xenophobic cyber crimes were proposed in 2002. The Convention did not necessarily guarantee that the issue of cyber crime would have an immediate solution. The provisions could come into full effect only if they were approved by that country's national legislature. Despite all of the controversy surrounding the Convention and the surveillance powers given to the nations who adopt it, the treaty is still a step ahead in the capturing and prosecution of cyber criminals. Since then, a plethora of laws have been adopted across the different countries of the world reinforcing them against the threat of cyber crime. Illegal or unauthorized use of a computer system, theft of private data and digital fraud are considered acts of felony in the US. Organizations without a viable network security program can be held responsible for negligence in the event of a cyber attack.

Keywords: Cybercrime, Legislation, Digital.

INTRODUCTION

Cyber crime is an international problem, with the UK public, business and government being targeted by criminals outside the UK as well as within. National Governments cannot solve this problem alone, and while Governments can regulate within their own borders, they cannot regulate externally. There is a need to ensure that countries are able to support the fight against cyber crime, and that there are international standards for operational work. International co-operation is most easily facilitated where different legislative systems have common offences which allow for the investigation and prosecution of an offence regardless of the jurisdiction it may have been committed in or wherever the evidence of an offence may be located. Common offences also allow for the possibility of extradition by providing for dual criminality requirements.

One commonly experienced difficulty is in making requests for data to other law enforcement agencies or data owners outside the UK. This process varies in its success, speed and complexity dependent on the country, or more frequently the company concerned. Many exchanges are facilitated by personal contacts or the reputation of the organization or individual requesting the data. The success of a request is not always dependent on whether a country has signed an international Convention or agreement which indicates it will provide the co-operation sought. The UK works closely with other countries, including through the G8, EU and the Council of Europe to set these standards. In the arena of child protection, international law enforcement cooperation has been successfully established, despite some of the differences in law and approach between countries.

The Legislation on Deregulation of Telecom Industry

To protect consumers' interests and market competition, Telecommunications Act 1984 stipulates that Telecom administration should perform a range of duties, including top and specific duties such as promotion general responsibility and community needs. The chief functions of Telecom administration are to improve the interests of citizens and consumers in

***Corresponding Author:** Jitender K Malik Email:

related market, and to promote market competition. Hence, Telecom administration has specified a serious of tasks, mainly related to the improvement of citizens' rights and interests, for the promotion of competition. Telecommunication administration, while performing its duties, should respect the rights and interests of consumers as to their choices of goods, price, service quality and etc.

The 1984 Act has set up an independent telecommunication regulation institution, OFTEL with the function of regulating domestic telecom operation together with the Minister of Trade and Industry. 1981 started the separation of the British post and telecommunications, signaling the start of BT commercialization. 1984 Act enacts the privatization policy and the BT privatization, selling its 51% stake.[1] It is regarded as an important historic milestone on the history of British telecommunications. In 1991 British Telecom (BT) industry, fully opened, is equipped with single or multiple telecoms regulator. In 2003, BT set up the post of telecommunications ombudsman for the justice of consumers, in charge of consumers' complaints of fixed and mobile networks.

The Legislation on Telecom Competition

In the nineties, the British telecom policy ended the oligopolistic monopoly, and started the overall opening of BT markets. To better the rights and interests of consumers and to improve market competition, United Kingdom enacted Competition Act in 1998.[2]The Act includes 71 items, dealing with four kinds of legislations. The first chapter of Competition Act is to prohibit competition items in competition agreement, and the second chapter is to emphasize the banning of protocols and decisions that have bad effects to UK trades, the writing off decisions that impede, distort and limit the domestic competition of UK among businesses or enterprise confederation. The prohibited provisions formulate that these protocols and decisions are invalid.

The second chapter of the Competition Act regulates the abuse of authority: if any one or more industries led to the abuse of dominant market position resulted in bad effect of UK trade, it or they should be cancelled; such behavior resulted to abuse should be cancelled as (a) unfair sell or buy directly and indirectly, (b) limiting technology to the anticipation of consumers, and (c) putting the trading party at a competitive disadvantage.[3] Telecommunication administration in 2003 set up the general terms and conditions, including 21 items. These clauses specify the rights and obligations of suppliers, which are regarded as the reference framework of new decision and disputes.

The Legislation on Intellectual Property

British copyright system is in constant development in the past few centuries, whose scope is far beyond the kinds of books. 1956 Copyright Law enlarged the scope of protection of intellectual property rights.[4] UK enacted the Patent Law in 1977 so as to make the European patent approved throughout UK. The Patent Act specifies that the patent right can be empowered to the product inventor or process innovator on the condition that the product is newly invented, innovative, and applicable to industrial development. The 1988 Copyright has provided a legal foundation for copyright design and patent law including the written or other forms of recording work such as computer derivative works. And the 1992 legislation has enlarged that of 1988. The literature amendment includes database, computer program previously prepared by programming information. On January 1, 1998, the new intellectual property law was established in the UK.

The Legislation on Electronic Transactions

The UK consumer contract legislation is also complete though earlier. The Unfair Contract Terms Act, 1977 contains provisions for commercial contracts for the supply of software. It provides further that the resources which he could expect to be available to him for the purpose of meeting the reliability should it arises; and how far it was open to him to cover himself by insurance. The Supply of Goods and Services Act, 1982 implies requirements that the supplier should exercise reasonable skill and care and that any goods ultimately supplied will comply with identical requirements relating to title, ultimately comply with identical requirements under the Sale of Goods Act, 1979.

The Consumer Protection Act, 1987 is involved in product concepts, the definition of product defects, legal liability and remedy, litigation and defense. The Act specifies that defects are due to its security under the general consumer expectations and that manufacturers are responsible only for the loss of defective products to its consumers. The Protection Act is to introduce the aspects of consumer protection from personal injury, property damage led by the responsibility systems, and the implementation of the law to maintain the interests of consumers which is regarded as the legal guarantee of relief by the consumers.[5]

The Legislation on Privacy Protection

The Data Protection Act was enacted in 1984 for protecting information and data. The new edition of Data Protection Act, published in 1998, put forward eight personal data protection principles such as the fairly and lawfully processed personal data, personal data obtaining for specific purposes, adequate but not excessive data, accurate data, specific purpose confined data, processed data under this Act.[6]

The Legislation on Computer Misuse

The Computer Misuse Act was enacted in 1990 to make provision for securing computer material

against unauthorized access or modification; and for connected purposes. A person is guilty of an offence of "unauthorized access" if: (a) he causes a computer to perform any function with intent to computer secure access to any program or data held in any computer; material. (b) the access he intends to secure is unauthorized; and (c) he knows at the time when he causes the computer to perform the function that that is the case. The intent a person has to have to commit the offence need not be directed at— (a) any particular program or data; (b) a program or data of any particular kind; or (c) a program or data held in any particular computer. A person guilty of the offence shall be liable on summary conviction to imprisonment for a term not exceeding six months or to a fine not exceeding level 5 on the standard scale or to both.[7]

Any person guilty of 'unauthorized access with intent to commit or facilitate commission of further offences' shall be liable— (a) on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both; and (b) on conviction on indictment, to imprisonment for a term not exceeding five years or to a fine or to both.[8] Unauthorized modification of computer material is also punishable. Here, the requisite intent is an intent to cause a modification of the contents of any computer and by so doing— (a) to impair the operation of any computer; (b) to prevent or hinder access to any program or data held in any computer; or (c) to impair the operation of any such program or the reliability of any such data. The intent need not be directed at— (a) any particular computer; (b) any particular program or data or a program or data of any particular kind; or (c) any particular modification or a modification of any particular kind. For the purposes of these provisions, the requisite knowledge is knowledge that any modification he intends to cause is unauthorized.[9]

Cyber Law in the United States

Cybercrime laws have developed with frequent reference to property law. Statutes such as the Computer Fraud and Abuse Act (CFAA), 2000.[10] and the Digital Millennium Copyright Act (DMCA), 1998 [11] create rights akin to a property owner's right to exclude. E-mail and voice mail that reside on a remote server receive substantially less protection than they would receive if they were stored at home. Thus, while the property metaphor has expanded the protection of intellectual property, data that resides on a computer in one's possession, and computer users and resources against intruders, this has led, practically speaking, to less protection for an increasing range of communications. An important factor in determining the government's ability to search communications and data is the ownership of the computer hardware that stores or transmits the data. Most Internet users store significant amounts of data on remote computers, which effectively reduce barriers to government acquisition relative to the physical counterparts of identical data. [12]

The Substantive Law of Cybercrime

The Wire Fraud Statute being the first law used to prosecute computer criminals in the USA. It was seen that the communication wires were used in international commerce to commit fraud. To overcome such US passed the Law so as to prohibit the use of communication wires. This was an effective statute as it was to overcome defrauders trying to obtain money, property by false representation or promise; modus operandi being radio or television communication, signs or signals.[13] This statute was successfully used in 1970's and 1980's to convict government officials of defrauding the public of its intangible right. In a paradigmatic case Governor Marvin Mandel of Maryland was convicted of mail fraud for promoting certain legislation beneficial to the owners of a race in violation of his obligation to render the citizen of the state fair and impartial service free from bribery.[14] The era witnessed technological progress so this Statute suffered certain limitations the wire fraud statute was written without computer crime in mind and as such it has serious limitations when dealing with it, not all computer related crimes can be prosecuted with it, not every crime committed using a computer is done with the intent to commit a fraud, and not all computer crimes use interstate or international wires. [15]

The Computer Fraud and Abuse Act (CFAA), 1984

Existing laws did not extend so readily to threats to computer systems as they did to threats against people or the value of copyrights. Early efforts to apply theft and trespass laws frequently failed, yet the temptation in many legislatures to apply a property law structure to computer system access proved strong. From this failure of imagination at the federal level, the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 (CFAA) [16] was born. The CFAA defines a variety of civil and criminal violations arising from "accessing a computer without authorization or exceeding authorized access."[17] Despite strong criticism that the CFAA's failure to define "access"[18] renders it incoherent and broader than intended, the CFAA remains the statute of choice in a broad range of criminal computer misuse cases.

One of the most typical roles of the CFAA is in the prosecution of virus, worm and Trojan horse writers. In a particularly disruptive and expensive episode, David L. Smith, who created and released the "Melissa" virus in 1999, was sentenced to twenty months in federal prison. Smith's conviction points to the breadth of the meaning of "unauthorized [19]access" that the landmark case of *United States v. Morris* [20] established: exploiting a weakness on one system can give rise to a massive number of unauthorized accesses to other systems, a phenomenon rather remote from the real property underpinnings of many unauthorized access statutes. The vision of property rights that underlies the CFAA not only remains intact but could

become even stronger. The day may soon be at hand when it will be possible to violate both the CFAA and the Digital Millennium Copyright Act (DMCA), 1998 during a single access of a copyrighted work.

The Economic Espionage Act (EEA), 1996

Congress has realized that keepers of trade secrets, like proprietors of computer systems, often have an interest in exercising the power to exclude. It has responded by offering protection that is partly colored by a property right. The Economic Espionage Act,[21] the first federal statute to protect trade secrets, defined two crimes: (i) *economic espionage* and (ii) *theft of trade secrets*. These crimes differ primarily in the beneficiary of the misappropriation. 'Economic espionage' outlaws appropriation of a trade secret with the intent or knowledge that the appropriation will benefit a foreign power.[22] The trade secret theft statute[23] bans identical conduct but does not require a foreign beneficiary of the misappropriation.

The most striking provisions in the EEA are the identically worded §§ 183 1(a)(2) and 1832(a)(2), which create criminal liability for a person who "without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys a trade secret." In contrast to state civil trade secret misappropriation statutes, which generally require that the secret be obtained by "improper means," the EEA takes a more property-based approach by making the authorization by the trade secret owner, or lack thereof, the basis for liability. Moreover, in contrast to most states' provision of civil remedies, the EEA provides only criminal remedies.[24]

The EEA's criminal provisions and property-based themes represent a legislative endorsement of an approach that prosecutors and private plaintiffs had tried to advance, but which faltered when the misappropriation of "purely intellectual property" was at issue. In *United States v. Brown*,[25] for example, defendant John Brown escaped prosecution under the National Stolen Property Act (NSPA)[26] because Brown's former employer had shipped the alleged trade secrets, a computer program and software manuals from a former employer, to Brown on backup tapes that Brown himself owned. The Tenth Circuit affirmed dismissal of the case, holding that the NSPA "applies only to physical 'goods, wares or merchandise' that were themselves 'stolen, converted or taken by fraud." Without protection for the information itself, prosecutors face a gap in the criminal law. The federal wire and mail fraud statutes, moreover, cannot "completely close the enforcement gap," because these statutes apply only when the victims of trade secret misappropriation are permanently defrauded of their information. Although the Supreme Court suggested that a trade secret could form the basis of a legally cognizable property interest that suggestion fell far short of creating a broad right that would allow federal prosecutors to intercede in cases of nascent appropriation.

The EEA may have overfilled this gap by defining crimes that could overlap with both the NSPA and with various intellectual property crimes. In June 2002, for example, two individuals pled guilty to theft of trade secret counts for stealing and transporting across state lines chemical reagents that were used in immune suppression research.[27] This activity might have been cognizable under the NSPA. Similarly, the Justice Department obtained a guilty plea from Robert Keppel, whom it accused of § 1832(a)(2) trade secret theft for purchasing, and subsequently selling *via* a Web site, copies of Microsoft certification exams.[28] The Keppel case could mark a shift in prosecutions for cases that implicate copyright's reproduction and distribution rights.

Trade secret charges when applicable could prove more attractive than copyright, because the act and *mens rea* requirements for trade secret misappropriation are easier to meet. There is no need to engage in the sometimes messy task of proving copyright infringement, nor does § 1832 require prosecutors to prove that the accused acted for "commercial advantage or private financial gain." As the Keppel case shows, works may be protected under both the EEA and copyright law, but the EEA may obviate the need to stay within the "precisely defined limits"[29] of the Copyright Act's criminal provisions. At the time the Court wrote, these provisions at least reflected the difference between ownership of a copyright and "the possessory interest of the owner of simple goods, wares or merchandise, to prosecute copyright crimes. As applied to Keppel, however, the EEA's provisions embrace both the rhetoric[30] and the legal effect of real property. Previously unable to persuade courts to expand intellectual property protection on theories of "unjust enrichment" or "restitution," and certainly unable to convince courts to expand criminal penalties beyond existing statutes, federal prosecutors now have at their disposal a trade secret law whose operative language is more expansive than state trade secret laws. Although this approach potentially creates grounds for challenging a statute as being unconstitutionally vague, no such challenge against the EEA has prevailed. [31]

The Digital Millennium Copyright Act (DMCA), 1998

The justifications for assigning liability on the basis of unauthorized access to computer systems, or the use of trade secrets "without authorization," are less apparent in the context of copyrighted works, where wide dissemination of works is an important goal of copyright law.[32] Congress did create such a right with the DMCA. Once again, the complexities of digital

computers-this time, their capacity to make and distribute perfect copies of works at almost zero cost-led Congress to augment criminal copyright liability with a form of ex ante liability based upon circumventing the "digital walls"[33] that may protect a work. This shift in copyright law from *ex post* enforcement to *ex ante* control raised general concerns; the arrest of Russian programmer Dmitry Sklyarov[34] for alleged DMCA violations caused outrage.[35]

This first test of the DMCA's criminal provisions resulted in an acquittal,[36] but *United States v. ElcomSof*[37] has still affirmed that the DMCA supplies copyright holders with a powerful right to exclude unwanted users from accessing their works. The government based its charges against Sklyarov and his employer, Elcom, Ltd. ("*ElcomSoft*"), on their allegedly production' and marketing of the Advanced e-Book Processor (AEBPR). The government alleged that the primary purpose of the AEBPR was to "remove any and all limitations on an e-book purchaser's ability to copy, distribute, print, have the text read audibly by the computer, or any other limitation imposed by the publisher." On the basis of these capabilities, the government categorized the AEBPR as a technology that circumvents "rights controls" rather than a technology that circumvents an "access control"' measure, such as a password. Some of the features that ElcomSoft advertised in connection with the AEBPR included "Advanced PDF Password Recovery," however, so the AEBPR arguably had the potential to be an access control circumvention technology. Moreover, eBooks, like DVDs, are encrypted, and thus use a technological measure that falls within the meaning of section 1201(a). Finally, since ElcomSoft sold the AEBPR, the alleged violation of sections 1201(b) (1)(A) and 1201(b)(1)(C) formed the basis for the criminal charges against it.

ElcomSoft demonstrates that United States copyright law now provides criminal punishment not only for "bad acts" but also "bad machines."' In its defense, ElcomSoft argued that the statutory definition of which machines are "bad" is unconstitutionally vague. Citing the textual differences between the access control circumvention ban in section 1201(a) and the rights control circumvention ban in section 1201(b), ElcomSoft urged the court to consider that section 1201(b) defines "no underlying substantive provision,"' which "renders it impossible to determine which tools [section 1201(b)] in fact bans."

The court rejected this constitutional challenge.' Addressing ElcomSoft's argument that section 1201(b) provided no useful standard to determine which devices circumvent usage control measures, the court held that "all tools that enable circumvention of use restrictions are banned, not merely those use restrictions that prohibit infringement." This holding marks a pronounced shift in copyright law from *ex post* enforcement to *ex ante* control. Not only does the DMCA protect Adobe e-Books from devices "primarily designed"' or "marketed"' to circumvent an e-Book's usage control measures, but it does so before any devices has been alleged, let alone proven, to have violated "a right of a copyright owner."

Although the DMCA provides some exemptions from the act-of-circumvention ban,' and creates a safety valve from the circumvention ban, commentators have questioned whether these exemptions will do much to qualify the absolute property right that would formally exist without them. The criminal charges against ElcomSoft, as well as the civil lawsuit against distributors of an unauthorized DVD decryption device, have continued to make the DMCA unpopular among computer professionals and have even prompted some legislators to call for reform. In addition to illustrating how broad the DMCA's circumvention device bans are, ElcomSoft also possesses considerable symbolic value. It represents the first test of the government's willingness to punish makers of devices that threaten the "digital walls" around digital works, and thus to enforce the legal prong that copyright holder have asserted is necessary to support technological measures used to guard commercial works.[38] A copyright holder can distribute a work to the public with access controls and usage rules-that is, with the exclusive attributes of physical property-and the government will sanction activities that might undermine the enforcement of this exclusivity.

The Children's Internet Protection Act (CIPA), 2000

Internet filtering laws in the United States are mostly introduced at the State level,[39] although federal legislation has been introduced for schools and libraries – The Children's Internet Protection Act (CIPA), 2000. Typically, internet filtering laws in the United States are concerned with protecting minors. Laws apply to schools and libraries, although some States also require publicly funded institutions to apply controls to block the accessing of pornography, obscene and other harmful material by minors.

However, legislation is now being considered to force vendors or suppliers of Internet-enabled devices to implement Internet filtering technology by default. The aim is not to prevent adults from accessing pornographic material on their personal devices, only to ensure that there are some controls in place. That means all vendors/suppliers of Internet-enabled devices will be required to implement a web filtering control, with the new device owners required to opt in if they wish to view pornography. Opting in must be done in writing and requires proof of age. Consumers will also be required to pay a fee to have the Internet filtering software removed.

At the federal level, all schools and libraries are required to comply with CIPA and implement web filters to prevent minors from accessing obscene material, pornographic images, images of child abuse, and other potentially harmful material if they wish to apply for discounts under the E-rate program or accept Library Services and Technology Act grants. If organizations choose not to apply for those grants or receive E-rate discounts, Internet filtering laws in the United States do not apply, at least at the federal level.

Internet filtering laws in the United States are applied at the State level and usually concern K12 schools and public libraries. Not all states require Internet filters to be applied. Some only require policies to be introduced to restrict access. Individual States have introduced legislation requiring schools and libraries to implement web filters or policies to control the content that can be accessed by minors. When policies are required to control access, schools and libraries may prefer to use a software or cloud-based solution to provide a greater level of protection. State laws are only concerned with ensuring the minimum level of Internet safety for minors when venturing online.

When the United States Supreme Court upheld the constitutionality of the Children's Internet Protection Act, [40] the legal challenge centered on the way the statute was written. The Supreme Court's decision states that the wording of the law does not place unconstitutional limitations on free speech in libraries. But, the decision did not address the constitutionality of the *application* of the law in public libraries and school libraries. As such, the Supreme Court decision upholding CIPA does not foreclose future legal challenges to CIPA. In fact, some of the opinions in the case by Justices who upheld the law actually encourage future legal challenges if the application of the law creates limitations on free speech for adults.

Typically, when the Supreme Court decides an issue, their decision is the final word on a legal issue. However, the decision in this case is unusual in that the case only decided the text of the law did not include provisions that, based on the way in which they were written, would clearly infringe on the First Amendment right of freedom of speech. The decision did not address whether the application of the law would also avoid infringing on constitutionally protected rights of free speech. Future legal challenges to CIPA, if they occur, would be based on the *application* of the law in public libraries and could potentially be raised by library patrons or by professional library organizations.

the views of four Justices and two separate concurrences that each represented the view of a single Justice. The two Justices who each wrote a separate concurrence both based their upholding of CIPA very specifically on the text of the law, not its application. These two concurrences openly acknowledge the assumption that CIPA will not place inappropriate burdens on patrons and will not prevent the exercise of protected free speech activities in public libraries by adults. Justice Kennedy wrote, however, that if some libraries cannot unblock Web sites or if "it is shown that an adult user's election to view constitutionally protected Internet material is burdened in some other substantial way," then CIPA should be challenged in its application. The application of CIPA in public libraries may persuade the two concurring Justices that the decision does significantly limit constitutionally protected free speech. In such a case, the balance of the Supreme Court on the issue could shift significantly. This situation opens the door for legal challenges to CIPA as it is applied in public libraries based on the burdens it places on adult patrons' ability to access constitutionally–protected free speech using the Internet.

The implementation of CIPA in public libraries has the potential of raising a wide range of First Amendment issues. Depending on the circumstances in individual libraries, many potential grounds for legal challenges to the constitutionality of the application of CIPA could arise. These challenges all relate to the fact that CIPA could significantly reduce the amount of free speech that adult patrons could access through the Internet in public libraries. This decision regarding the constitutionality of CIPA raises a number of legal concepts related to the First Amendment that may prove to be of considerable importance to public libraries in the United States in any future legal challenges to the application of CIPA. These challenges may be able to demonstrate that the effects of CIPA–mandated filtering and other applications of the law restrict the abilities of patrons, especially adults, to access constitutionally protected free speech.[41]

US Procedure

When electronic communications play a role in a criminal investigation, however, a property-based analysis leads in exactly the opposite direction. Extending the Fourth Amendment's guarantees of security in one's "persons, houses, papers, and effects" to communications that do not fit easily into any of these categories requires judicial determination. Other information to which a person might wish to restrict the government's access receives only the protection that a relevant statute, if any, offers. As electronic communications become more important in daily life, on the one hand, and a more important means for criminal investigation and intelligence surveillance on the other, these limitations are likely to become more widely noticed.

An odd dynamic has developed; the Supreme Court's extension of Fourth Amendment beyond a

property-based concept, to activities surrounded by a "reasonable expectation of privacy," did not dispose of the role of property in determining the level of protection that a given communication receives. Ownership of property is as important as ever; the ownership and physical state of computer equipment determines the showing that the government needs to conduct a search.

The Fourth Amendment

A pair of 1967 Supreme Court decisions initiated the application of Fourth Amendment[42] protection beyond the property-based standard[43]in the text of the amendment. In *Berger v. New York*,[44] the Court invalidated New York's eavesdropping statute on the grounds that its "broad sweep resulted in a 'trespass intrusion' into a constitutionally protected area."' In *Katz v. United States*,[45] the Court broadened Fourth Amendment protection from this explicitly property-based conception to one that incorporated a conception of a right to privacy. In his concurrence in *Katz*, Justice Harlan stated what has become the guiding principle for the constitutionality of a search: a search is unconstitutional if it violates an individual's: (i) "actual (subjective) expectation of privacy" and (ii) "the expectation is one that society is prepared to recognize as 'reasonable."

Katz, however, narrowed Berger by holding that electronic surveillance, if brief, narrowly focused, and approved in advance by a judge, could be constitutional. Subsequent cases began to limit this expansive view of the Fourth Amendment. In *United States v. Miller*,[46] the Court held that business and banking records "lack any legitimate expectation of privacy," once they are given to a third party, "even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." In *Smith v. Maryland*,[47] the Court applied Miller and held that there is no legitimate expectation of privacy in the information that pen registers collect. Determining the level of protection that a given form of communication should receive is a task that continues to bedevil Congress and the courts.

Statutory Framework

In Title III of the Omnibus Crime Control and Safe Streets Act of 1968, ("Title III" or the "Wiretap Act"), Congress codified the Supreme Court's holding in *Katz*. The Wiretap Act also illustrates, however, that the protections of the Fourth Amendment do not easily translate to new technologies, absent application of the Fourth Amendment by the Supreme Court. Congress has taken some measures to maintain the balance between advances in technology and the potential "evisceration of Constitutional rights"'[48] that technological advances could effect. The resulting body of electronic surveillance law is complex. The same laws govern State and private conduct and simultaneously provide civil and criminal penalties. Changes enacted under the USA Patriot Act (USAPA)[49] further complicate the statutes.

Title III and the Electronic Communications Privacy Act (ECPA)

Title III bans wiretapping by the government except in investigations of enumerated crimes,[50] and only after showing a neutral magistrate that ordinary investigative techniques are ineffective.[51] Title III also requires that investigators minimize the data that they collect and provides procedural opportunities to object to evidence collected in a wiretap before it is introduced into a criminal trial.[52] In its original form, however, Title III applied only to the interception of a "wire communication," which is "any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception,"[53] or an "oral communication."[54]

When computer-based communications became more common, Congress expanded Title III protection to "electronic communications."[55] In Title I of the Electronic Communications Privacy Act, 1986, Congress created statutory protection for electronic communications in transmission, including "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo-electronic or photo-optical system that affects interstate or foreign commerce."[56] Thus, the ECPA extended protection to electronic **c**ommunications , but did so by creating a separate category of communications based on the underlying medium of transmission.

The distinction between wire and electronic communications is important because Title III provides a suppression remedy for illegally intercepted wire communications,[57] but not for illegally intercepted electronic communications.[58] It is also worth re-emphasizing that Title III applies only to the interception-the acquisition of the contents of a communication contemporaneous with transmission[59] of wire and electronic communications; but Title III does not apply to communications in storage. Recognizing that this gap left the increasing volume of non-voice and electronic communications without Fourth Amendment or Title III protection, Congress created in Title II of the ECPA protection for stored electronic communications.[60]

Until Congress passed the USAPA, wire and electronic communications became "stored" at different times. Specifically, an electronic communication entered electronic storage when "a copy of a communication is created at an intermediate point that is designed to be sent on to its final destination." The USAPA left this definition unchanged but altered the

classification of voice mail. Whereas voice mail used to be a wire communication "in transmission" until its recipient listened to it, and so was protected by Title III's suppression remedy, the USAPA placed all voice mail within the ambit of Title II of the ECPA. Thus, investigators' failure to obtain the proper warrant for voice mail can no longer serve as a basis for exclusion of that evidence.

Underlying the ECPA's approach to regulating government access to e-mail, account records, or subscriber information,' is the fact that the relevant communications are almost always stored on a computer that is not the property of the recipient of the relevant communication, or to whom the data subscription data pertains. The baseline of protection is therefore not the Fourth Amendment's guarantee of security in a person's papers or effects, but rather the rule of third-party possession, which makes unreasonable the expectation of privacy in a communication held by a third party.

Although this result makes sense in terms of the history of third-party possession, it is incongruous with the laws discussed herein. The CFAA creates the rough equivalent of a criminal trespass statute with respect to intrusions against the owner of the computer. The DMCA criminalizes penetrations of the "digital walls" around copyrighted works, no matter where they are stored. The reliance of Internet users upon third parties for almost all aspects of their activities, however, excludes them from such strong, property-based protection, regardless of the prevalent perception of e-mail as deserving of Fourth Amendment protection.

Judicial Anticipation of the USAPA

Despite the obvious relevance of Title III and the ECPA to criminal investigations, the differences in the statutory language regarding the interception of wire and electronic communications were first explored in civil cases. In *Steve Jackson Games v. Secret Service*,[61] the Fifth Circuit was the first court to squarely confront the disparate treatment of wire communications and electronic communications. The Steve Jackson Games court held that "an intercept requires participation by the one charged with an 'interception' in the contemporaneous acquisition of the communication through the use of the device.' Absent explicit inclusion of storage of an electronic communication in the definition of the communication, in a manner parallel to that of wire communication, the Fifth Circuit held that interception, and thus the Title III warrant requirements; apply to electronic communications only as they pass over the wires from one computer to another.

The Ninth Circuit was the next court to confront this issue, and in *Konop v. Hawaiian Airlines*,[62] the court expressed its agreement with the holding in Steve Jackson Games. The court, applying Title III and the ECPA as they stood before passage of the USAPA, noted that Congress, through the USAPA, "accepted and implicitly approved the judicial definition of 'intercept." Thus, beginning with the notion that Konop's website was somehow his "property" would be seriously misleading. Although Congress has given statutory protection to most forms of electronic communications, those communications are not protected as ordinary property. Instead, a complex body of surveillance law, in which the ownership of the equipment on which the communication resides, plays a deciding role. Simply put, a home page is not like a home with respect to government searches and surveillance.

Australian Cybercrime Legislation

In August 2012, the Australian Government passed the Cybercrime Legislation Amendment Act, 2012 (CLAA). The purpose of the CLAA was to enable Australia to accede to the Council of Europe Convention on Cybercrime (Cybercrime Convention, 2001), the only international treaty on cybercrime. Although Australia already complied with many of the Cybercrime Convention provisions, the CLAA means that Australia now meets all of the Cybercrime Convention requirements for members, including the obligation of telecommunication carriers to preserve data and meta-data. The CLAA should bolster the ability of Australian law enforcement agencies to prevent, investigate, and prosecute cybercrime offences. However, the CLAA is a reminder of the increasing threat cybercrime poses to Australian companies, including corporate espionage, data theft, business interruption and reputational damage.

The Cybercrime Convention is an international response to the borderless nature of cybercrime. For example, a criminal based in Eastern Europe can steal Australian credit card data from the website of an online business based in South-East Asia. The vast bulk of cybercrime, particularly targeting Australian companies, originates off-shore, and is often the result of well-organised and resourced organisations. Many of these criminal organisations are based in, or utilise ICT facilities based in, states with poor legislative or enforcement frameworks. This makes it virtually impossible for any state acting alone to locate or apprehend the responsible parties, or even to gather evidence about what occurred, and how.

The stated aim of the Cybercrime Convention is: “to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation”. The Cybercrime Convention encompasses offences against computer data and systems, computer-related forgery and fraud, content-related offences, and infringement of intellectual property rights. The Cybercrime Convention

also requires member states to provide mutual assistance to other member states. As well as harmonising national laws, the Cybercrime Convention aims to facilitate the sharing of intelligence, and to make it easier for member states to collect evidence from foreign jurisdictions.

Australia's federal cybercrime offences are contained in the Criminal Code Act 1995 (the Criminal Code), and were actually based on the Cybercrime Convention. They are divided into two main groups: offences relating to telecommunication services[63] and computer offences.[64] The Criminal Code contains a number of offences relating to the unauthorised access, modification, or impairment of data and restricted data.[65] The CLAA broadened the scope of these offences. Prior to the CLAA, the offences required the relevant data to be owned by the Commonwealth, held by, or on behalf of, the Commonwealth, or that the access, modification or impairment was caused *via* a carriage service. The CLAA removes these limitations, so that any unauthorised access, modification, or impairment of any data is now an offence. This captures situations where employees modify data on-site without authorisation, or use local networks to conduct such acts.

Before the CLAA, the Criminal Code created an offence for causing unauthorised impairment of an electronic communication to or from a computer, but only if the authorised impairment was caused through the use of a carriage service or the electronic communication was sent to or from a computer owned by the Commonwealth.[66] The CLAA amendments (based on the federal Parliament's constitutional power to enact legislation with respect to external affairs, including in order implementing an international treaty or convention) now mean that any unauthorised impairment is an offence, regardless of how it occurs, or where the communication was being sent to or from. This expands the illegality of any conduct which diverts or redirects communications with a computer, including during a distributed denial of service (or DDOS) attack.

Also, the CLAA amended section 478.2 of the Criminal Code. Prior to the CLAA, it was only an offence to cause unauthorised impairment of the reliability, security or operation of data on a computer disk, credit card, or other storage device, if that device was owned by the Commonwealth. The CLAA removed that restriction, so that it is an offence to conduct such acts to any such device.

The CLAA Also Amended Three Other Acts:

- The Telecommunications Act, 1997 relating to the obligation of carriers to preserve stored data and meta-data;
- The Telecommunications (Interception and Access) Act, 1979 relating to the scope of telecommunication interception powers; and
- The Mutual Assistance in Criminal Matters Act 1987 relating to the cooperation powers of Australian law enforcement agencies with their foreign counterparts.

Although most of the amendments from the CLAA commenced in 2012, the changes to the Criminal Code only came into force on 1 March 2013.

Legislation in Poland

Computer crime and cybercrime are not legal notions in Poland. These terms do not appear in the body of substantive criminal law at all. An ancillary definition of "cybercrime" is provided by the Minister of Justice regulation concerning the European Arrest Warrant.[67] It has a narrow meaning referring to acts against the protection of computer data which are gathered, stored, processed or transmitted in the information system. Criminological definitions usually have a broader meaning and are used as an umbrella term that covers all crimes related to computer data, committed against, on and/or throughout information systems, including computer networks, especially the Internet.

As opposed to the Council of Europe Convention on Cybercrime,[68] the Polish Penal Code does not comprise a definition of the terms "computer system" or "computer data", despite the fact that such terms are used in a description of cybercrime offences.[69]

The said definitions are also not covered by the Act of 2008 aimed at unification of computer terminology in the Polish legal system.[70] A more general problem, still under discussion in Poland in the context of constitutional law, concerns a direct application of definitions laid down in the ratified international conventions by the courts.

As in most other countries, computer crime legislation in Poland has a relatively short history. It started to be drafted by the Criminal Law Reform Commission as an integral part of a new penal code in the early 90's.[71] First public debate on computer crime problem took place on the occasion of an international conference "Legal aspects of computer-related abuse," organized under the aegis of the Council of Europe in Poznan in 1994. Three years later, most of computer-related infringements that compose "a minimum list" of the 1989 Council of Europe recommendation were criminalized under the Polish Penal Code of 1997. This code represents a "young generation" of the European criminal codes that went into force already in the Information Age.

Perhaps for this reason, its specific part contains a chapter entitled "Offences against the

Protection of Information," which corresponds with the proposal set forth in the literature by Professor Ulrich Sieber. Originally, this chapter has included four types of offences against *confidentiality*, *integrity* and *availability of computer data* and systems.

These Were:

- Data espionage[72]
- Computer eavesdropping[73]
- Data interference;[74] and
- Computer sabotage[75]

A number of specific provisions, such as those on computer fraud[76] unauthorized reproduction of a protected computer program[77] handling of illegally copied software[78] and telecommunication fraud[79] were included into the category of offences against property.

A legal definition of document[80] has also been extended in order to make prosecution of computer forgery possible. In addition, such specific ICT-related offences like computer espionage[81] and causing a general hazard as a result of interference with automatic data processing[82] were introduced to the Penal Code. The list of computer offences has expanded in size pursuant the 2004 amendment of the Penal Code. This legal change was related to accession of Poland to the European Union and it was aimed at harmonization of Polish criminal legislation with the Council of Europe Convention on Cybercrime.[83]

In effect, three new CIA offences: system interference,[84] misuse of devices,[85] and data interference[86] were introduced[87] to the Penal Code. Simultaneously, the possession of child pornography was prohibited and a wording of some already existing provisions on computer-related offences was slightly modified by inserting the term “computer data” instead of “information,” or “the record on an electronic information carrier.” Intended implementation of the Council of Europe Convention on Cybercrime has also affected procedural regulations. Some specific procedural measures envisaged by the Council of Europe Convention on Cybercrime were incorporated into the Code of Criminal Procedure. The most recent legal change of cyber criminal law took place in 2008 in order to implement the regulations contained in two Framework Decisions to the legal system of Poland. This goal was accomplished in the case of criminalization of hacking[88]and the so called virtual child pornography[89] in the Penal Code.

Offences against the Confidentiality, Integrity, and Availability of a Computer System and Availability of a Computer System

All offences against computer security are within chapter XXXIII of the Penal Code, (“Offences against the Protection of Information”). This chapter includes eight basic provisions[90] protecting the main features of information security, i.e., confidentiality, integrity and availability. Besides traditional offences against secrecy of the State[91] and other official secrecy[92] there are penal provisions related to offences defined in the Council of Europe Convention on Cybercrime[93] as the crimes of illegal access,[94] illegal interception,[95] data and system interference[96] and misuse of devices.[97] Polish Penal . Code provides a wide range of offences that specifically relate to a computer system and data as the objects of offending.

The Following Offences Against Confidentiality, Integrity And Availability Of Computer Data And Systems Can Be Distinguished:

- Illegal access to a computer system[98]
- Illegal interception[99]
- Data interference[100]
- System interference[101]
- Misuse of devices[102]

Most of CIA offences are prosecuted upon the complaint of the injured person. So the criminal proceedings cannot be initiated without the injured person lodging a complaint with a State prosecution office. Since that moment these offences are prosecuted *ex officio*. However, the injured person has a right to change his decision and can withdraw a complaint before a trial begins, provided that the public prosecutor consents. Only computer sabotage[103] and misuse of devices[104] are the offences prosecuted *ex officio*, i.e. pursuant public accusation. Under the legality principle, to which the Polish criminal justice system formally adheres, the police and prosecutors have a duty to investigate and prosecute all known offences and offenders. One should note that the Penal Code defines an offence as "a socially harmful act" prohibited by the criminal law. This definition allows the police and the public prosecutor to have *de facto* discretion on the decision of whether a minor act is considered a formal violation of the law, to be labeled an offence and prosecuted.

REFERENCE

1. British Telecom, Annual Report (2001), p. 72
2. With effect from March 1, 2000
3. Article 19
4. British Telecom, Annual Report (2000), p. 46
5. Yang Songcai, “Reviews of UK Consumer Protection Law” 3 Consumer Economics, 36-38 (2003)
6. OFTEL, Annual Report (London: HMSO, 2000), p.65
7. Section 1
8. Section 2
9. Section 3
10. 18 U.S.C. § 1030 (2000)
11. Pub. L. No. 105-304, 112 Stat. 2860 (1998) (codified in scattered sections of 17 U.S.C.)
12. Aaron Burstein, A Survey of Cybercrime in the United States, 18 Berkeley Tech. L.J. 313 (2003)

13. Legal Information Institute (LII); 18 USC 1343-Fraud by Wire, Radio, or Television 1988. 113-36
14. Aaron. D. Hoag, "Defrauding the Wire Fraud Statute: United States v La Macchia" 8 (2) Harvard Journal of Law and Technology 511 (1995)
15. Rajlakshmi Wagh, "Comparative Analysis of Trends of Cyber Crime Laws in USA and India" 2(1) International Journal of Advanced Computer Science and Information Technology 42-50 (2013)
16. Pub. L. 98-473, 98 Stat. 1837, 2190 (Oct. 12, 1984) (codified as amended at 18 U.S.C. § 1030 (2000))
17. 18 U.S.C. §§ 1030(a)(1)-(5) (2000)
18. The CFAA does define "exceeds authorized access," but not in a way that helps determine when access occurs, or by what means authorization is to be ascertained.
19. Press Release, CCIPS, "Creator of Melissa Computer Virus Sentenced to 20 Months in Federal Prison" (May 1, 2001)
20. 928 F.2d 504, 510-11 (2d Cir. 1991) (holding that individuals with some authorized access to protected computers could still be liable for acts of "unauthorized access")
21. Pub. L. No. 104-294, 110 Stat. 3488 (Oct. 11, 1996) (codified at 18 U. S. C. §§ 1831-1839 (2000))
22. A research scientist was alleged to have stolen genetic research materials from the Cleveland Clinic Foundation and to have transported them to RIKEN, a research institute operated by the Japanese government. Press Release, CCIPS, Scientist Pleads Guilty to Providing False Statements Regarding Trade Secret Theft from Cleveland Clinic Foundation (May 1, 2002),
23. 18 U.S.C. § 1832 (2000)
24. The penalties can be quite severe. Economic espionage is punishable by a maximum fine of $500,000, or 15 years in prison, or both. 18 U.S.C. § 1831 (a)(5). Trade secret theft is punishable by a maximum fine of $5,000,000, or 10 years in prison, or both. Ibid. § 1832(a), (b)
25. 925 F.2d 1301, 1307 (10th Cir. 1991)
26. Ch. 645, § 1, 62 Stat. 806 (1948)
27. Press Release, CCIPS, Pair Charged With Theft Of Trade Secrets From Harvard Medical School (June 19, 2002)
28. Press Release, CCIPS, Former Vancouver, Washington, Resident Pleads Guilty to Theft of Trade Secrets from Microsoft Corporation (Aug. 23, 2002)
29. Dowling v. United States, 473 U.S. 207, 217 (1985)
30. Section 1832 is entitled "Theft of trade secrets" and defines the requisite mens rea for a violation as "intent to convert a trade secret."
31. See, e.g., United States v. Krumrei, 258 F.3d 535, 536 (6th Cir. 2001) (holding that the EEA's definition of "trade secret" in 18 U.S.C. § 1839(3) was not unconstitutionally vague as applied to defendant).
32. Jitender K Malik, Dr. Sanjaya Choudhury A Brief review on Cyber Crime - Growth and Evolution, Pramana Research Journal, 2019, 9(3), 242- 278.
33. Malik, J.K., & Choudhury.S. (2018) PolicyXZ. *International Journal of Recent Scientific Research*, 9(12)pp. 29811-29814.
34. Malik,J.K.,(2018).Cyber-crimes- policy in India, *International Research Journal of Human Resources and Social Sciences*, 5(4) 554-565.
35. Lawrence Lessig, "Jail Time in the Digital Age" N.Y. Times (July 30, 2001), At A17
36. Matt Richtel, "Russian Company Cleared of Illegal Software Sales" N.Y. TIMES (Dec. 18, 2002), at C4.
37. United States v. Elcom Ltd., CR 01- 20138 (N.D. Cal. 2001)
38. See Dean S. Marks and Bruce H. Tumbull, "Technical Protection Measures: The Intersection of Technology, Law and Commercial Licenses," 46 J. Copyright Society U.S. 563, 563-64 (1999) (explaining that both technological and legal protections are necessary to prevent the unauthorized duplication and distribution of digital works).
39. In South Carolina, legislation has been proposed that would require consumers to pay $20 to have the pornography block removed. The legislation was filed with the South Carolina General Assembly in December 2016. Similar legislation was also proposed in Utah in 2016.
40. United States v. American Library Association, 539 US 194 (2003)
41. Paul T. Jaeger and Charles R. McClure, "Potential legal challenges to the application of the Children's Internet Protection Act (CIPA) in public libraries: Strategies and issues" 9 First Monday 2 (2004)
42. U. S. Constitution Amendment IV states, in its entirety:
43. The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.
44. Frank J. Eichenlaub," Comment, Carnivore: Taking a Bite out of the Fourth Amendment?" 80 N.C. L. Rev. 315, 334 (2001)
45. 388 U.S. 41 (1967)
46. 389 U.S. 347 (1967)
47. 425 U.S. 435 (1976)
48. 442 U.S. 735 (1979)
49. United States v. Scarfo, 180 F. Supp. 2d 572, 583 (D.N.J. 2001)
50. Uniting and Strengthening America by Providing Appropriate Tools Required to the Intercept and Obstruct Terrorism, Pub. L. No. 107-56, 115 Stat. 272 (2001)
51. 18 U.S.C. § 2516
52. Ibid. § 2518(3)(c)
53. Ibid.§ 2518(5)
54. 18 U.S.C. § 2510(1)
55. Oral communication' means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation." Ibid. § 2510(2)
56. teve Jackson Games, Inc. v. Secret Serv., 36 F.3d 457, 460 (5th Cir. 1994) (citing the prohibition on intercepting an "electronic communication" in 18 U.S.C. § 2511 (a))

57. 18 U.S.C. § 2510(12) (2000)
58. Ibid. §§ 2510(11), 2515, 2518(10)(a)
59. § 2518(10)(c)
60. 18 U.S.C. § 2510(4); Steve Jackson Games, 36 F.3d At 460
61. Title II of the ECPA is also known as the Stored Communications Act (SCA)
62. Konop v. Hawaiian Airlines, 302 F.3d 868, 874 (9th Cir. 2002)36 F.3d 457, 460 (5th Cir. 1994)
63. 302 F.3d 868, 874 (9th Cir. 2002)
64. Part 10.6
65. Part 10.7
66. Sections 477.1, 477.2 and 478.1 of the Criminal Code
67. Section 477.3
68. Regulation of the Minister of Justice of 20 April 2004
69. on the European Arrest Warrant, Journal of Laws 2004, No.73, item 664
70. Article 1
71. The National Office of the Public Prosecution Service is in favour of implementation of Article 1 of the Convention into the Polish Penal Code. Such a position has been taken by this highest unit of the Prosecution Service during the consultations on ratification of the Council of Europe Convention on Cybercrime (Memorandum of 23 May 2008, PR I 078-53/08).
72. Law of 4 September (2008) on Standardization of IT-related Terminology in the Laws, Journal of Laws, No.171, item 1056
73. Kazimierz Buchala in Ulrich Sieber (ed.) Information Technology Crime National Legislations and International Initiatives (Carl Heymans, 1994), p. 382
74. Article 267 § 1
75. Article 267 § 2
76. Article 268 § 2
77. Malik, J.K., & Choudhury.S. (2018), Cyber Space-Evolution & Growth. *East African Scholars Journal of education, Humanities and Literature*, *2*(3), 170-190.
78. Malik, J.K., & Choudhury.S. (2019) A Brief Review On Cyber Crime -*Growth And Evolution. Pramana Research Journal*, *9*(3)-242.
79. Choudhury, S., & Malik, J.K. (2018). Policy Considerations in India against Cyber Crime. *International Journal of Recent Scientific Research*, *9*, (2), 29811-29814.
80. Malik, J.K., & Choudhury.S. (2018).The Criminals In A Cyber Environment Using Computer Networks. *International Journal of Current Innovation Research*, *4*(12), 1416-1422.
81. Malik Jitender K And Sanjaya Choudhury, Cyber Crimes- Policy In India, International Research Journal Of Human Resources And Social Sciences, Volume 5, Issue 04, April 2018, 554-565. Article 115 § 14.
82. Article 130 § 2
83. Article 165 § 1 point 4
84. Ulrich Sieber, "The Legal Aspects of Computer Crime" (Report at The Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders Havana, Cuba August 27–September 7, 1990), p.16
85. Article 269a
86. Article 269b
87. Article 268a
88. Article 202
89. Jitender Kumar Malik and Sanjaya Choudhury, PolicyXZ. International Journal of Recent Scientific Research, 9(12), pp. 29811-29814.
90. Jitender K Malik, the criminals in a cyber environment using computer networks, International Journal of Current Innovation Research, Vol. 4, Issue, 12(A), December, 2018, pp. 1416-1422,
91. Kirkorian, Wartella & Anderson, "Media and Young Children's Learning" 18 Future of Children, 39-61 (2009)
92. Plowman, McPake & Stephen, "Just picking it up? Young Children Learning with Technology at Home" 38 Cambridge Journal of Education, 303-319 (2008) Articles 265-269b
93. Article 2
94. Article 3
95. Articles 4 and 5
96. Article 6
97. Article 267 § 1 and 2
98. Jitender k malik, cyber crimes- policy in India, International Research Journal of Human Resources and Social Sciences, Volume 5, Issue 04, April 2018, 554-565.
99. Articles 268 and 268a.
100. Articles 269 and 269.