Pungency in the Amusement

Radha Kuruwitabandara
Faculty of Law, General Sir John Kotelawala Defence University, Ratmalana, Sri Lanka
radhiguit@gmail.com

***Abstract*—** *This research paper intends to discuss the negative impact of cellular phones in the perception of cellular phone crimes. Today the increasing rate of so said crimes is seen to be considerably high parallel to the development of technology in cellular phones. The technology of cellular phones has been developed from the simplest feature phones to smartphones by which that fact itself has contributed to increase of usage of cellular phones. Similarly, the rate of cellular phone crimes too have increased. But it is seen that the contemporary problems are not well addressed by the contemporary laws. It has been the main objective of conducting this research to provide few recommendations on amending the existing law on cellular phone crimes.*

***Keywords*—** *Cellular phone crimes, Sri Lankan law, Lacunas*

I. INTRODUCTION

A cellular phone, also called a mobile phone sometimes, is a type of short wave analogue or digital telecommunication in which a subscriber has a wireless connection from a mobile phone to a relatively nearby transmitter. The transmitter's span of coverage is called a cell.

A cellular phone crime as regarded in this research is a wrongful act committed with a wrongful intention in a situation where a cellular phone is either a tool or the target or both. Further, a cellular phone criminal is a person who commits a cellular phone crime.

This research paper will proceed to analyse the effect of cellular phones on the creation of the idea of cellular phone crimes, the social factors of Sri Lanka which has provided a helping-hand to such crime rate, the role of Sri Lankan law in its operation and the emerging trends in the global arena.

II. CELLULAR PHONES AND CRIMES

The use of cellular phones in human lives has become so vital that even the morning alarm is being replaced by a cellular phone. The definition of cellular phones itself contains a wide scope because the concept of cellular phone has been gradually developed into many deviations. For an example, the development of feature phone to the smartphone has further expanded its scope to tablets, electronic notebooks and such similar versions. This makes it more complicated in the matter of narrowing down the research area. But in comparing the nature of those with cellular phones, it is clear that each one of them should be incorporated into the definition.

Moving further to the rate of usage of cellular phones in Sri Lanka in contrast with the rate in the world as a whole, it is essential to look into few statistics. By 2014, more than one quarter of the global population are cellular phone users. It is 6.8 Billion in a number. By 2018, it is expected to be increased to 69.4%, which will exceed the half-line[173]. By the end of 2012, Sri Lanka had an estimated 20.3 million of mobile phone users out of 20.8 citizens[174].

There are many reasons for this gradual increase of usage. The inexpensive prices of some models of cellular phones have transformed it to an ordinary item rather than an exciting one. Cellular phone companies in the other hand are observed to be very frequent in releasing new updates of their productions which has then resulted in creating a bigger second-hand market which fits low budgets.

Moving into the core aspect of this essay, aforesaid usage rate has a direct connection with the increasing crime rate related to cellular phones. Despite of all the development experienced, one most important factor is being ignored, the security. It is rather a social factor, that as it has been available for people in low economic standards and with less education, the possibility of them getting involved in misuse of cellular phones is higher.

Even the definition of cellular phone crimes stands as provided previously, one would yet have a confusion between computer crimes and cellular phone crimes. That is because, today it is a common fact that smartphones with a network connection can perfectly act as a computer, or even more sophisticated than that. And all the portable internet provider gadgets are working on

[173] eMarketer report on Worldwide Mobile Phone Users.
[174] Mobile mania in Sri Lanka by Charitha Ratwatte

a cellular phone network. Moreover, several parts of cellular phones are considered in cyberbullying, which is mainly a computer crime.

Cellular phones today are equipped with Bluetooth, wireless fidelity (WiFi), Third generation technology (3G), global system for mobile communication (GSM), General Packet Radio Service (GPRS), virtual private networks, dial-up-service and many other advanced services. These make it possible to network mobile devices at home, a workplace or even on the go.

What is to be understood is that the decisive factor is the technology used to transmit the call, irrespective of the phone's capabilities and inabilities. Standing on this factor helps to draw a line between cellular phone crimes and cybercrimes.

III. CELLULAR PHONES OPENING DOORS FOR CRIMES

A.Cellular phone crimes as cyber crimes

It was previously discussed that cellular phones have now evolved to act more as portable computers than just a phone which makes calls. This has created a link between cellular phones and cybercrimes. What this has further resulted in is the absence of knowledge of being a victim and sometimes even being the wrongdoer. They tend to hold the idea that the fact of not using a computer in that particular act provides them an exception for not being a criminal or a victim, in which they actually are. Every person who uses internet, Bluetooth, or even infra-red enabled cell phones can be easily put into the sphere of cybercrimes. Thus it is clear most of all the phone users has the possibility of becoming a subject of a cybercrime.

B.Few common cellular phone crimes

Bluebugging is an attack done on a cellular phone through a Bluetooth connection[175], which is a very common offline mode of connecting two or more devices. Despite the benefit of quick transformation of data, a stranger might have the opportunity of getting into ones' private cellular phone. This access allows the stranger to take over the total control of the victim's phone. The danger is even crucial because unless the original user is known enough about his device, he cannot even recognise that the phone is being hacked. The hacker can access to almost all the information in the victim's phone. He can reach the extent of making calls and listen to other conversations that occur through the infected phone.

Phishing is getting revealing and access to personal information such as passwords and credit card numbers and use of such information for fraudulent practices[176].

Vishing is a way of committing financial crime by a phone. In other words this is voice phishing[177]. This has come into play through the practice of using cellular phones for online shopping and bank transactions. These are similar to phishing attacks which includes identity theft such as credit card information. A misleading phone call can fulfil all the necessities of the hacker.

Smishing usually happens through the Short Message Service or more commonly known SMS. User is sent with a lucrative message requiring them to disclose his personal information which the hacker misuses later. This can end up in information theft.

Malware is another vital threat to cellular phones. Once infected, the device perform malicious activities. This can happen through a simple short message (SMS), a file transfer or downloading programmes from internet[178].

C.Cellular Phone Crimes in Sri Lanka

Some upholds the idea that, as for the fact that Sri Lanka is still a developing country, most of those very advance, mastermind cellular phone crimes do not occur in Sri Lanka. But one may not conclude that for the fact of not having reported incidents. It is disappointing to note that even the Yearly all island crime evaluation done by the Police Department of Sri Lanka denotes no sign of cybercrimes or cellular crimes. The department only recognizes a very few types of cellular phone crimes mostly for the fact that they are not reported in the frequency the occur. They are, Phishing and pharming for identity theft, Lottery scams and phone number scams.

Identity theft is one of the most frequent ones out of all in Sri Lanka. An identity theft is when someone's professional information is stolen to commit a fraud[179]. In theses, most of the times, the victim receives a message appears to be from a credible, real bank or credit card company, with links to a website and a request to provide account information. But the website is fake, made to look real.

[175] Oriyano, S P. (2013) *Hacker Techniques, Tools and incident handling*, p.199, 2nd ed, Jones & Bartlett Publishers

[176] Phishing *https://www.microsoft.com/security/online-privacy/phishing-symptoms.aspx*

[177] Vishing *http://www.lifelock.com/education/smartphones/vishing/*

[178] Malware *http://blog.avast.com*

[179] Police Department Records, Sri Lanka

Lottery scams are another popular type seen in Sri Lanka. In these, it includes scams which can go under the name of a genuine lottery. Unsolicited messages or telephone calls tell people they are being entered into a prize draw. Later, they receive a call congratulating on winning a substantial prize. But before claiming the prize they are said to pay an amount of money to pay for administration fees and taxes. The prize of course does not exist. It is quite clear that no genuine lottery would ask for a money back from a winner. But some people fail to track such factors[180].

Phone number scams are a type that has been there for a long time, and still in use. These are at first send as postal notifications of a win in sweepstake or a holiday offer. These include an instruction to ring a premium rate number. This is generally a 900 toll number. So said prizes do not exist[181].

Above mentioned are a very few offences committed with the use of cellular phones in Sri Lanaka, which are stated according to the records as reported to the Police department. There should be no doubt that there are failed and unreported complaints. And it is very clear that the advancement of new ways of committing crimes will never look back for the law to follow it. In fact the development of technology has been a helping hand for offenders.

D.Latest legal trends regarding cellular phone crimes

The world as a whole has now come to the conclusion that an advance legal system should be implemented in eliminating the crimes committed via cellular phones.

Offences relating to cellular phones can be addressed in two major ways. It can either be addressed as a claim of civil damages or in the point of a crime. The matter in question is the criminal aspect. In regarding it as a crime, imposing a punishment can be the ultimate result of the proceeding which would mostly be a fine or an imprisonment.

Many of the countries have taken necessary steps to introduce new laws to their legal systems through their legislative bodies considering the crime rate that is spiralling out of control.

E.Indian legislation on Cellular phone crimes

Republic of India, the closest neighbour to Sri Lanka enacted the Cell phones and the Information Technology Act in the year 2000.

Section 2 (i) has defined the devices covered by the Act as "any electronic, magnetic, optical or other high speed data processing device or system which performs logical, arithmetic and memory functions by manipulation of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software or communication facilities which are connected or related to the computer in a computer system or computer network". It is therefore clear that a mobile cell phones are just been made a part of it.

Section 2 (r) refers to the term 'electronic form', which means any information sent, generated, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device. In fact, the transformation transactions done through a cellular phone are encompassed into this Act.
Section 43 deals with destruction and unauthorized access to information technology devices.

Section 66 provides protection against hacking. Hacking is defied in regard to this section as any act with an intention to cause wrongful loss or damage to any person or with the knowledge that a wrongful loss or damage will be caused to any person. An offender could be given with an imprisonment of three years or a fine.

Section 67 (A) sets out the punishment for transmitting of material containing sexually explicit act or conduct in electronic form. According to this, an imprisonment up to five years or a fine.

A protection against confidentiality and privacy of data is provided under the section 72.

Along with the IT Act, section 378 of the Indian Penal code is incorporated. This particular section relates to Theft.

F. Is the Indian Law sufficient to address the cellular phone crimes in India?

It is clearly seen that many of the crimes committed by use of a cellular phone eventually leads to the information theft. Even if India has the Cell phones and the information technology act enacted, there is no specific Act for Data protection as seen in United Kingdoms. Supporters defend the arguments of reality stating that the Information Technology Act has enough provisions for data protection in which the reality is far beyond. The said Information Technology Act provides

[180] Police Department Records, Sri Lanka

[181] Police Department Records, Sri Lanka

aids to a certain extent but not as it is required by the necessities.

The legislation in existence is seen to be defending very few and common crimes which does not accommodate the whole sphere of cellular phone crimes. For instance, it was earlier discussed that a cellular phone crime can be committed either by a phone with a network connection or without such. It is only the equipped phone that has been taken to consideration in this enactment. For example, bluebugging can result in a crucial damage to ones' information. But there are no provisions provided to cover such matters. The concern has solely been aimed on cellular phones with connection networks which has neglected all the other possibilities. Therefore it is clear, even if there is an Act on cellular phone crimes in India, it is even not sufficient enough to address the varied possibilities.

G. Data protection Act 1998 – United Kingdom

The data protection Act of United Kingdom is an Act to make new provisions of the regulation for the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information as per to its preamble. Simply, this Act governs how the personal data of an individual is used by organizations, businesses and the government. This Act basically gives a right of access to personal data to the individuals. Personal data is collected when an individual takes part in a purchase of a good or service from a company or any other service provider. It is regarded as a breach of a civil right to use someone's confidential information for fraudulent purposes. The Data Protection Act was enacted as a guideline to be followed by the companies in the scope of gathering personal data in extending possibilities.

Section 1(1) defines the scope of data controller as to who needs to comply with the Act. Such data controllers should be responsible for the availability, integrity and security of the data that fall under the Act.

In discussing about the Data Protection Act, there are eight main requirements which the Act is expected to consist. In other words they are the core expectations of the Act. They are, information must be processed fairly and lawfully, information must be processed for limited purposes, information must be adequate, relevant and not excessive, information must be accurate and up to date, information must not be held for longer than is necessary, information must be processed in accordance with the individual's rights, information must be kept secure and information should not be transferred outside the European Economic Areas unless adequate levels of protection exists.

Out of these requirements, the one that says that the information must be kept secure is indicating a relevance to that of loss of data and data theft through mobile phones. This section extends to impose duty on a company who is holding or using data of an individual to keep such data in a secured manner. In a situation where a company loses a Computer with such data, the Act provides provisions to impose a liability on that company. Furthermore, the Act also takes steps to fine organizations who act in such negligence. This Act indirectly insists the Companies to not to be careless. The company must ensure that the personal information are in safe hands and will not be passed to wrong hands.

The matter in question is whether the losses occurred by a cellular phone is acceptable in relation to the Data protection Act. The Data Protection Act covers 'personal data' and 'sensitive personal data'. Personal data is any information about an individual irrespective of the format of the information[182]. This means information that affects the person's privacy. 'Sensitive personal data' are the information that includes the individual's race, religion, political beliefs, mental health and other similar information[183]. The Act does not cover confidential data of every nature but only the ones that contain personal data. This seems to be a gap in the law.

It is clear that this Act does not cover every aspect of loss of data. In fact, it only covers the loss of data occurred in the possession of a company or such other organization. But it is satisfactory to a certain extent that it covers at least a part of it. Sri Lanka in the process of achieving legislative goals, it would be useful to have enacted a Data protection Act including the aspects of cellular phones as well.

H. Sri Lankan legislations on cellular phone crimes

It is disappointing to state that Sri Lanka has not yet taken steps on addressing cellular phone crimes as a separate area of law.

Sri Lanka has only a Computer Crime Act No 24 of 2007 which is precisely addressing the Computer crimes but not the cellular phone crimes. The definition of the term computer is given in the interpretation section of the Computer crimes Act as "an electronic or similar device having information possessing capabilities"[184]. One may

[182] Section 1(1), Data Protection Act of 1998, UK

[183] Section 2, Data protection Act of 1998, UK

[184] Section 38,Computer Crimes Act no 24 of 2007, Sri Lanka

argue that this definition has the possibility of considering cellular phones. But in moving into the other sections of the said Act it is seen that the legislature had not possessed the intention of recognizing and incorporating cellular phones or crimes related to such devices in enacting Computer crime Act, No 24 of 2007.

In relation to computer crimes, this act has discussed unauthorized access to computers (S. 03), intentional use of a computer in a manner of affecting the national security, national economy or public order (S. 06), buying, possessing or selling unlawful data (S. 07), and unlawful accessing to a password or access code of a computer (S.09). It is beyond certainty that all the foresaid crimes could also be committed in relation to a cellular phone. It is therefore a major loophole to not to have a body of law to govern the said area.

Apart from that, there are also some crimes that can only be committed by cellular phones as discussed earlier in this text, which are unable to be committed by use of a computer. It is in question how such issues are to be regulated.

In regard to the context of India, these crimes can be addressed by the Penal Code of Sri Lanka under the offence of theft to a certain extent.

Section 366 of the Penal Code of Sri Lanka is as follows;

"Whoever, intending to take dishonestly any movable property out of the possession of any person without that person's consent, moves that property in order to such taking is said to commit 'Theft'."

The term 'movable property' should be precisely taken into account. Section 20 in the General explanations of Chapter II of the Penal code refers to movable property.

"…includes corporeal property of every description, except land and things attached to earth…"

This definition only covers theft of property of corporeal nature. Corporeal nature needs the subject matter to be physical and tangible. It is obvious that a collection of data in the software mode is not tangible. But a collection of data stored in a compact disk or a floppy disk or a pen drive can be considered as included into this definition since it becomes a movable property once the data is stored in a movable device. In that matter, it is applicable to an extent, the Penal section of 366 for the instances where a cellular phone with a data collection is the subject of theft.

In considering the different types of cellular phone crimes, it is clear that a mere theft of the cellular phone is not the only mode of such crimes. There are far more advance modes of accessing only to the data storage even without the victim's knowledge. This results in a stranger accessing to the intangible data of another person without reaching the tangible device. The existing law in Sri Lanka does not seem to cover or recognise such gains or losses of data in particular. This is a major lacuna identified in this particular area. The failure of penal law of Sri Lanka on cellular phone crimes could be well elaborated on this fact. For instance, the other Penal code section that shows an applicability to an extent is the section 21.

S. 21 (1) Wrongful gain – "gain by unlawful means of property to which the person gaining is not legally entitled."

S. 21 (2) Wrongful loss – "loss by unlawful means of property to which the person losing it is legally entitled."

A person who makes access to another's data on a cellular phone gets a wrongful gain which is not lawfully entitled to him. The Victim, in the other hand, suffers a wrongful loss of data which ought to be possessed by him in legal means.

Even though the sections stands so, it is in question whether they can make an influence towards the rapid growth of cellular crime rate in Sri Lanka.

I. Analysis

As long as there is no existing legislation found in the area of cellular phone crimes in Sri Lanka, the need of an implementation of such a law is in greater necessity. In such an implementation, having regard to the laws of aforementioned countries would support such implementation to reach an advanced level of defending such crimes.

The particular commissions should be made recognized by setting out their constituent elements as it would contribute in imputing liability. Identification and providing a procedure to investigate and prevent cellular phone crimes should be the main purpose to be served. Punishment for commission of such crimes should be introduced further.

In regards to setting out a definition for these crimes, it needs a more comprehensive approach in comparison to that of the Indian Act on Information Technology. In the Indian Information Technology Act it seems to be an indirect reference to cellular phones rather than a direct definition. This has the possibility of creating loopholes in the practical use of the law.

Furthermore, the need of having defined the different forms of committing these crimes should also be laid down. As for an example, the acts of bluebugging and phishing are two particular acts that need unique recognition and also result in different degrees of damage. In that matter, it is essential to recognize the different types of cellular phone crimes under an umbrella definition.

The victims should also be empowered with a mechanism to claim damages for the data loss occurred due to the wrongful acts done through cellular phones.

These are the main aspects that need to be addressed in an implementation of a legislation regarding wrongful acts committed with the use of cellular phones.

XI. CONCLUSION

It was discussed previously that the law relating to cellular phone crimes in India is not competent enough to address the threats that are being created so far along with the vast development of technology. Comparatively, in Sri Lanka, where the law on cellular phone crimes is still in its infancy requires a greater attention and consideration than that of India.

The necessity should firstly be identified and then the findings should be addressed accordingly. An amendment to the Computer crimes Act No. 24 of 2007 can be raised by suggesting to incorporate cellular phones into it would be a practical recommendation at least as a primary step to be taken.

The time that has been passed without an enactment should not be considered as a failure but as an extra extension of time in which the neighboring countries have kept their first step so that we are able to follow them along with upgrades to the lacks they possess. In fact, this is the best stretch of time for Sri Lanka to lead its legal system to the digital world with a comprehensive enactment.

It is reasonable not to have the best solution at the first attempt itself. But taking the first step today would eventually lead to its own improvements parallel to the technological evolution.

ACKNOWLEDGMENT

The author is grateful to Mr. Buvaneka Aluwihare PC. Justice of the Supreme Court for the valuable suggestions and the guidance provided, and Mr. Prasantha De. Silva Justice of the Civil Appeal court, Gampaha. for the massive academic support rendered. Further, the assistance given by Ms. Bhagya Wickramasinghe is also gratefully remembered.

REFERENCES

Cell Phone Crimes – India, <*http://www.legalindia.com/* >

Computer Crime Act, No. 24 of 2007

Data protection Act 1998 of United Kingdom, *www.legislation.gov.uk*

Data protection; *www.gov.uk; www.clouddirect.net*

Gupta N A. Mobile cell phones and cybercrimes in India. <*http://www.legalindia.com/* >, Accessed 06.16.2015

Oriyano, S P. (2013) *Hacker Techniques, Tools and incident handling*, 2nd ed, Jones & Bartlett Publishers

Jayasinghe K G (2012). *Computer and Internet law*

Malware., <*http://blog.avast.com*>

Mobile technology crime. Accessed 06.16.2015, < *http://police.mizoram.gov.in/* >

Penal Code of India 1860

Penal code of Sri Lanka, No. 02 of 1883

Phishing.,
<*https://www.microsoft.com/security/online-privacy/phishing-symptoms.aspx*>
www.google.lk/search?hl=en&redir_esc=&client=ms-android-sonymobile&source=android-launcher-widget&v=141400000&qsubts=1435156652850&action=devloc&q=what+is+phishing+attack#hl=en&q=define+phishing

Reed C. and Angel, J. (2000). *Computer Law*, 4th ed, Universal Law Publishing Co. Pvt. Ltd.

Sri Lanka Centre for cyber security
http://www.slcert.gov.lk

Smith R G. Preventing mobile telephone crimes., *http://www.aic.gov.au/media_library/conferences/other/smith_russell/1996-10-crf.pdf* >Accessed 06.16.2015

Vishing.,
<*http://www.lifelock.com/education/smartphones/vishing/* >

BIOGRAPHY OF THE AUTHOR

[1]Author is a law undergraduate of the General Sir John Kotelawala Defence University, Sri Lanka. She is currently studying in the second year.