INFORMATION, INFORMATION TECHNOLOGY, CRYPTOGRAPHY AND LAW

*Shanmughan D. Jayan**

I Information and information technology

FROM TIME immemorial, the value of information was identified. Creation, storing, transmission and retrieval of information was an important facet of system and various modes of accomplishment of the said functions were also present in the system. No revolutionary aspects were created that posed a threat to the thereto-existing modes of control of information. However, the latter half of the last century brought into existence information technology that ushered in a substantial change into this position. With the aid of this technology information of all forms was digitalized, and all the operations on any kind of information could be accomplished in that form. This became a revolutionary change and started to pose threat to the hitherto existing modes of control of information. The growth of information technology can be seen as unparalleled. In fact, the vertical and horizontal expansions of information technology have created a scenario whereby a good portion of the working of the society is exclusively residing in communication channel. A scrutiny of societal functioning will show that there basically exists only movement of man and material, and transmission of information. The latter part is being taken over completely by information technology. To condense the multilateral impact of this branch of technology is nothing but tremendous in infiltration, advancement and spread.

The transmission of information is an important facet of societal system. Newspapers, radio, television, office functioning, governance, teaching, telephone, speech, etc. thrive on this aspect. Information technology is directly dealing about information irrespective of its mode of perception. Due to this factor, information technology can integrate with all the above mentioned areas that are dealing with information. A conceptual examination from a different angle can provide another

* B.Sc., LL.M., Advocate, Kochi.

important aspect. All systems created or employed by man were either processing matter or energy. Information technology has created yet another system which is processing information, hitherto a task distinctive to man. This uniqueness and the pervasive nature of the technology is not leaving any field untouched and thus, unlike other technologies, this advancement is making its presence felt in all fields. In addition, the property of convergence ensures that nothing is left out. Further, internet is a freeway for information. In short, all these distinctiveness of information technology have made sure that all activities of the mankind are having or are aided by information technology.

The scope of information and its corresponding value has increased by leaps and bounds owing to the wholesome effect of information technology. Many times, the value of information is the efficiency of the owner in keeping it to himself. Unlike other tangible property, information can be multiplied within no time and thus diminishing or many times nullifying the value of the original one. In this context, the concept of information security gains significance. The concept as literally deducible from the terminology is nothing but securing of information. The relevance of securing of information is at the highest realm when it comes to that of internet owing to its inherent freeway nature. The predators of information are looking for information, and it is the duty of the information owners to make the information secure. Information in the communication channel or in internet is residing in all places or at no place. Unlike other tangible property, a casual sightseer is not having any notice of the demarcation of another's property which is in the form of information in communication channel. Thus information security in its minimal requirement should at least demarcate one's property from another's. It is doubtful whether such a demarcation is any sort of securing process. Fencing one's property is a normal recourse in physical world and without doubts it is a sort of demarcation. Drawing a line and putting a signboard are also common modes of identification of properties. If these processes can be termed as 'securing' there need not be any doubt on this point of securing information.

This minimum requirement of demarcating is the simplest form of securing of information. On the other end, highly complex methods can also be employed for securing information. When almost the global society's activities are being carried out by using the communication channel the need for protecting this communication channel is the aim of information security. There is need for protecting the information that is in a channel and destined to a receiver, as well as information that are residing in a system or network or even in a stand-alone system. Whether it is a simple demarcation or securing of the most complex kind, the tool

for that purpose is cryptographic methods.[1]

II Cryptography

Cryptography is the art and/or science of covert inscription.[2] This tactic or practice was known to human kind even from immemorial time or rather from the time of identification of value of information. The underlining factor for the use of cryptography is the inherent quest of human minds for maintaining secret.

Cryptography in its simplest form can be a shift of alphabets. For example, 'CAT' can be written as 'ECV', where E is used instead of C, C is used instead of A and V in place of T. Here the technique of shifting of alphabets can be cited as the algorithm and the number of shifting of position as the key.[3] Since the shifting is of changing two positions, the key is two. A key can also be some other number, for example, three. Then 'CAT' will be written as 'FDW'. So the sender or creator of the message will be sending the text 'FDW' instead of 'CAT' when he is using the shift of positions as three. The receiver will reduce the shift of alphabets by the same key and will read the message as 'CAT'. Here the process of converting the message into its coded form is known as encryption. The process of getting back the message is called decryption. The original message is known as plain text whereas the code message is known as cipher text.[4] Since same key is used for encryption as well as decryption, this type of cryptography is referred as single key cryptography.[5]

Shifting of alphabet's position is one of the easiest and earliest methods of encryption. There are so many other complicated techniques that are used for securing information in cryptography. Here, in the given example, the key is also simple in the sense that a number has been directly used for

1. Using this classical definition of cryptography, any sort of alteration in the information so as to make the perception more difficult can be qualified as use of cryptographic technique.

2. For details, see RSA Laboratories' Frequently Asked Questions About Today's Cryptography: Version 4.1, RSA Security Inc (2000). Available at *http://www.rsa.com*.

3. An algorithm is a set of rules that specify the order and kind of arithmetic operations that are used on specified set of data. These arithmetic operations could include such things as rounding rules, a logical decision or a specific formula. It is a computable set of finite steps to achieve a desired result. The word comes from the Persian author Abu Ja'far Mohammed ibn Mûsâ al-Khowârizmî who wrote a book with arithmetic rules (about 825 A.D). Key is the value that is used by the algorithm to encrypt and decrypt the data.

4. *Supra* note 2.

5. *Ibid*.

encrypting the messages. The key can also be made complicated by prescribing conditions. A condition can be laid down whereby the key is dynamic throughout the message. Suppose the condition prescribed is shifting of one position for the first alphabet and then to linearly increase it, then for 'C', the key will be one, for 'A' the key will be two, and for 'T' it will be three. Thus 'CAT' will be written as 'DCW'. Even though the technique is remaining as shifting the position of alphabets, key is coming with certain conditions. The security of cryptographic technique is directly proportional to the complicity of the method as well as key. From early stages of history of cryptography itself, the thrust was to improve the method as well as the keys. More the chances of deciphering the key and/or the method, the less were the security element of cryptographic technique.

The practice of using same key for encrypting as well as decrypting had many drawbacks. The receiver is always getting the chance of imposing as the sender because the receiver is getting the capability of the sender in as much as the key as well as the method used for encryption and decryption are one and the same. Suppose X is the sender of information and Y the receiver; and it is previously agreed that, so and so symmetric cryptographic method with a specific key will be used for encrypting the message. On receiving the message, Y will be using the same key or decrypting the message. Suppose in their group, there is another person Z who is also using the same key as well as method for writing messages between them. Now, Y will be able to make changes to the message received from X and he can very well send the same to Z using the same key as well as the method. Suppose Y is pretending as X in the message, there is no mechanism for Z for knowing who has sent it.

In addition to the simple method of alphabets, there are umpteen methods of simple key cryptographic techniques. Since identical key is used for encryption as well as decryption, these types of secret writings is also known as symmetric key cryptographic.[6] Using of pictures, symbols, complex mathematical equations, etc. are also examples of asymmetric crypto system. Whatever be the method employed, the above mentioned basic defect exists for symmetric key cryptography.

The concept of asymmetric cryptography emerged in this scenario.[7] The same is also known as private key, public key cryptography. Here, for

6. *Ibid*, the term symmetry is denoting that there is symmetry with respect to the key used for encryption as well as decryption; rather the keys employed are one and the same.

7. *Ibid*, as opposed to symmetric key cryptography, the key for encryption and decryption are different and hence the terminology asymmetric.

encryption, a particular key is used whereas for decryption another key is used. This key pair is related in such a complex form, thus the knowledge of one is not at all making anyone to know the other key.[8] Each person will be having his own unique key pair: Private key and public key. The private key will be known only to the owner whereas the public key will be made available to everyone. Taking the cited example, X can encrypt a message using his private key and send the ciphered message to Y. Y on receipt of the message can decrypt it using public key of X. Unlike the scenario detailed above with respect to symmetric key cryptography here Y cannot pretend himself as X and resend the message to Z. Because the private key of X is exclusively with him and only X can create or encrypt messages that can be decrypted using his public key. Thus one can observe that unlike symmetric key cryptography asymmetric cryptography is having certain definite advantages. There are further enhanced uses of asymmetric cryptography. If X wants to send message to Y and X wants to make sure that only Y reads it and also Y is to be sure of the sender of the message. Here X will encrypt the message by using his public key and will further encrypt the already encrypted message using Y's public key. Now even if anyone is getting the message only Y can decrypt it since Y's private key is required for decrypting. After the decryption using Y's private key what he is getting is an encrypted message done with X's private key. Now Y will have to further decrypt the message using X's public key. A successful completion of this will ensure that X is the actual sender.

One can theoretically see the potentials of cryptography. Used in an electronic environment cryptographic techniques prospects are just colossal. In information technology, use of cryptographic technique is unavoidable. This science of cryptography that was present from a very long time frame has suddenly come out into lime light as a great tool in electronic form of communication.

---

8. There are numerous algorithms for asymmetric encryption. The RSA algorithm remains the most famous one. Ron Rivest, Adi Shamir and Len Adleman of Massachusetts Institute of Technology invented RSA algorithm in 1978. The name RSA has been coined by taking the first letter of the first names of Ron Rivest, Adi Shamir and Len Adleman. The RSA algorithm relies on the difficulty of factoring immensely large numbers. In the key generation phase, the RSA algorithm generates a very large number usually 1024 bits long. This generated number is not just any number, but it is the product of two very large 512 bits long prime numbers. The security of the RSA algorithm relies on the difficulty of factoring this number to give the two large primes. That means 21024, which is approximately 10228 times the number of atoms in the universe. As a very small-scale example, imagine trying to factor 1261. A desktop computer could solve this in a fraction of a second, giving 97 and 13, but when the number in question is much larger, even supercomputers working together could not do it before the end of the universe.

III Cryptography and information technology

When one is pasting the envelope that is carrying the letter written by him, he is securing the information carried by that paper even though the envelope may be in a public channel. In electronic environment such a task needs to be mimicked so as to ensure that the paper is in a 'sealed envelope'. Technocrats identified cryptography as a tool to achieve this end. Due to the wide scale proliferation of applied information technology into the masses in a short span of time computing devices were becoming ubiquitous in the society. Thus information in electronic form became a need of general public also. This meant that there was need for public to rely on cryptographic techniques for securing their information. Cryptography used to be pet tool of espionage[9] and the same was usually associated with state, government, sovereign, etc. On the other hand, it was also used for rebellious activities. Thus cryptography which was hitherto a requirement of state, suddenly found itself to be a necessity for the pubic at large that are relying on electronic systems. Thus there was a sudden change in the usage pattern of cryptographic techniques. As mentioned earlier, the strength of the process of securing information using cryptographic technique is a direct function of complexity of the mathematical formula or equation employed. To what extent this complexity or making tough the cracking process of ciphered information can go is a perplexing issue. However, there exist certain intrinsically connected legal issues.

IV Legal issues

The citizens want cryptography for secret communication, whereas the state was hesitant in giving such an absolute right. State is always interested in knowing what is transpiring between the citizens and an alien, mainly citing larger interest of the state. When the citizens without any state intervention or control, deploy cryptography techniques the freedom of the citizen is enhanced which the state curtails for extracting information transpiring in the society. It is just like a written matter covered using an unbreakable envelop. The state is handicapped by this factor. Even if state knows that the information contained is against the interest of state, state can do nothing. Similarly, any doubtful information is also outside the reach of state. Thus for the larger interest of state, as a result of information technology there evolved the need for controlling

9. Chanakaya is said to have used cryptographic techniques in his fight.

cryptographic techniques.[10]

Even in highly democratic political environment it is a ground reality that the state is using its machinery for eavesdropping into the communication of its subjects. Telephone tapping, interception of postal materials, employing of spies are certain commonly employed state tactics of encroaching into citizens' private life; many times in the pretext of state interests. When cryptographic methods are used for private communication the state will be in an insecure position. The more the complex the cryptographic methods used more will be the difficulty of state for getting such information. Thus the issue will boil down to privacy of the citizen *vis-à-vis* state security. This issue seems to have been identified by the US long ago.

Cryptographic tools were considered as dangerous weapon in US[11] and there were control on its use and transactions. However, there was an outcry from the liberal people for the use of encryption as a tool for protecting the right to privacy in communication. The state was worried about the leakage of state secrets into the hands of potential state enemies. So there was, as usual, a fight between individual freedom and state security. In this situation the concept of clipper chip originated. Clipper chip idea was a compromise put forward by the federal government for protecting both the need for use of encryption at the same time upholding state security. Clipper chip was a hardware built into communication devices which encrypts the message at its inception and decrypts at its reception. Therefore, in the communication channel, the information will be in an encrypted form. So that the citizen's right to privacy of communication was recognised. Nevertheless, there was a negative side to this set-up. The state will be having access to all these encryption algorithms embedded in the clipper chips. The state authorities will be in a position to listen to any information that is passed between people. This suggestion from the federal government also raised strong criticism from right conscious people. In this context the idea of Trusted Third Party (TTP) originated. People are free to communicate using encryption but a middleman will be there who will be having a copy of the clipper chip and when circumstances require he will be disclosing it to the state. So that

10. The issue of use of cryptographic techniques in *Blackberry Phones* and the attempt of the Central Government to contain it is an example even though an isolated one.

11. In US, the federal statute Arms Export Control Act, 22 U.S.C. § 2778 has defined: "…[C]ryptographic (including key management) systems, equipment, assemblies, modules, integrated circuits, components or software with the capability of maintaining secrecy or confidentiality of information…" as on par with dangerous weapons.

the privacy of communication of individuals was guaranteed at the same time state interest was also given due importance.

The issue with respect to clipper chip was actually limited to that of telecommunication. However, the scope of use of cryptography in the present information technology is on a higher level and the chances of legal issues are also likewise. How far the system is ready enough to tackle the emerging issues? The author is of the opinion that this is the issue that is going to perplex the legal thinkers in future. There are certain latches in the identification of real legal issues and this is reflected in the prescription of remedies as well.

The role of certifying authorities in authentication process using digital signature[12] is one such example. Many countries have accepted digital signature as a mode of authentication and also recognized the role of certifying authority. One, who is examining the role of TTP in the light of the compromise formula as a result of clipper chip, can observe that unlike the common belief TTP is not the trusted third party of the contracting persons but it is enjoying the trust of the state. Role played by the certifying authority is actually an extension of the role of TTP. Thus, it can be seen that these agencies were evolved not because of the faith of the parties that were dealing with them, but because of the trust of the state. One should keep in mind the fact that in US, TTPs evolved due to the reason that there was control on cryptography. Whereas many countries that have accepted digital signature as a means of authentication, lack such a history. Thus speaking from principals certifying authority is not a necessity, as the so-called generation of trust is not the aim of certifying authority but it aims at security of state. As mentioned earlier, the creation of TTPs was a result of state interest in controlling the use of cryptography. Even in the presence of this known fact, legislatures throughout the globe are confusing things while they legislate on the area. This confusion and contradiction is actually an indication of the emerging issues.

The maximum employing of cryptography is going to be in securing of information in internet. To what extent cryptographic techniques can be used, how it should be used, who all can use it, etc. is going to be the core issue of the field. Existence of sovereign, territoriality, concept of property, relationships of real nature and paper-based transactions are certain basics upon which any legal system has placed great reliance. Many

12. A type of electronic signature for authenticating electronic communication and accepted in India *vide* Information Technology Act, 2003. The amendment cleared by the Houses of Parliament in the year 2008 has also brought in other techniques of authentication.

issues in connection with information technology are inherently lacking or are defying these basics. Even if one is identifying the above concepts the extracting of the required legal attributes is difficult to achieve. In real world, a societal system is contained or controlled vide four means, namely, by law, by social norms, by market conditions and by the nature of the system. These controlling factors also are not effective as far as information technology issues are concerned. The need of law for laying down the mode and modality of a system is always there and information technology is also not an exception. A perusal of the historical origin of legal control through strict prescription of compulsory mandates by the crown will reveal that in many circumstances, they were nothing more than state sanctification of prevalent practices of the society. Thus, laws controlling varied fields and subjects were nothing but continuation of practices. It is a fact that law lags behind technology, law encompasses the emerging challenges within its control and streamlines its growth in a manner acceptable to all. However, as far as this branch of technological advancement is concerned, it is strongly felt that due to its sudden growth law is not getting evolved but is being generated. When the system is trying to rely on earlier basics, as in the case of certifying authorities, it is creating contradictions. Infact, control creates order and this resultant orderly pattern only can assure minimal friction for a given system. This statement is true for any closed or open system. The smooth running of society at large is also achieved by this element of control. With respect to a political society this control is taken care of by the legal system. The dynamism of the society is having its impact on legal norms also and any change in behaviour of the society means some repercussions on legal system. This dynamism will be having many causes and technology is one among them.

Speaking generally as well as jurisprudentially the concept of property is of immeasurable significance and social, economic, legal and political issues with respect to the same had laid philosophical discussions. Thesis and antithesis as well as synthesis are plentiful surrounding this concept in all of the above-mentioned branches of thoughts. The extent of allowing property holding, how far property is extension of personality, what is the nature of property rights, etc. are debatable issues at any point of time. Nevertheless the need of protecting one's property was recognized and accepted by almost all political societies. Jurisprudential elucidation of this concept has been the pedestal of diverse branches of law in relevant treatment of various legal issues. Except in some legal issues, the reference of property is always to tangible real property. However, in the communication channel the whole scenario changes. In real world, property is having its own localization or demarcation. Thus even in the absence of

a specific notice each property is physically distinguishable. However in communication channel due to the absence of 'place' all property are residing in 'same place' or 'no place'. Else it can be termed that the actual location of residing of any 'information' is irrelevant. Or, otherwise, the physical demarcation existing in real world property is absent in communication channel.

While dwelling on the subject for giving an answer to the above-mentioned issue, another legal concept takes significance. Trespass is a very wide concept when discussed independently in this context. Trespass can be made on any property, the legal consequences and the defences being secondary. In a networked environment, all property is residing in 'same place' or 'no place'. So unlike real world the respective owner should identify each property because the very identification itself is creating different property due to independent existence of property. When examined minutely one can see that trespass is the first and foremost infringement. Thus protection of property can be achieved by avoiding trespass. This can be minimally by a mere notice or warning of the ownership and can be strengthened by using cryptographic techniques. Fatal methods like electrified fences had raised legal issues in protection of real world property. On the other hand, unless there is sufficient warning or notice different property will not be identifiable. Sometimes state will be interested in getting information of its citizens for state's interest. Thus how, why and when of usage of cryptographic tools is a legal concern.

There are many legal issues with respect to information technology, such as hacking, theft, fraud, privacy, piracy, misrepresentation, defamation, denial of service, etc. These legal issues are surrounded by a singular concept of concern, i.e., 'information'. A clear perusal of enactments deals with information and the juridical divisions present contradictions, when it is analysed from the conceptual angle. Take for example the two specific issues of hacking and theft; for the former an entry into some information is sufficient, whereas for the latter taking away of some information is required. One can see that both the issues are targeting information. While creating an enactment or rendering a decision on these issues, the legislature or the court as the case may be, are treating information both as immovable property and movable property. For the former, information is qualified with the attributes of immovable property whereas for the latter that of movable property. In some instances, 'information' is viewed as a unique concept. Thus there are evident incosnsistencies in different categories of issues. Further a fine perusal of issues of singular category also precipitates certain contradictions. This type of problems is more visible while courts examine the extent of infringement like how and when the rights of a person are infringed. To

sum up, legislated law as well as judge made law are showing a pattern that is not consistent while dealing about issues in information technology.

Authors from some quarters have mooted the idea that the concepts of property and trespass have to be infused or to some extent ameliorated for forming a jurisprudential basis for a proper treatment of legal issues. In the existing legal framework, one can neither identify as to what can be infringement nor the real nature of the concept of information. Cryptography remains to be the sole mode of bringing in some sort of control and/or protection of information in communication channel. However, cryptography is a technological advancement where law has never made an attempt to control hitherto.[13] So one can guess the problems that can ponder the legal system, as the paper world would be shifted to paper less world.

13. As mentioned earlier, United States example is an exception to this.