VOLUME 18 ISSN 2456-9704

DATA ENCRYPTION AND SURVEILLANCE

By Prabhjot Singh
From Fairfield Institute of Management and Technology

Abstract
Living around modern technologies comes with number of threats and cautious acts to be played by the individuals. In cryptography encryption means encoding a message in such a way that only authorized persons can use it and unauthorized persons are denied the access the main objective of encryption is to protect private information by putting it into a form that can only be read by people who have the access to use it whereas on the other hand Surveillance means by having watch on someone's act by different means such as cyber cells, intelligence beaureu's etc. Surveillance is mainly done to prevent crime activities taking place in the country by having an eye on the suspects.

Many a times whenever a person regardless of his religion, caste or community is suspected of something illegal by the authorities is kept under the process of surveillance so that the intelligence beaureu's can record their actions through their various branches which conducts investigation according to their own criteria.

For those who fear restrained government surveillance, encryption is an obvious technical response governments around the world are taking several measures to protect its public and to make their nation strong by introducing and regulating various structural reforms at regular intervals. A variety of technical and administrative measures have been also proposed to address law-enforcement and privacy concerns. Data privacy is the main concern for today's youth as number of activities are now regulated and conducted through technical devices and the structures that various portable or importable devices consist of. Gathering in large groups and connecting through social networking sites is also a serious concern and being strict towards such acts and cautious is as necessary for the youth as JOBS for today's young generation are. This research paper will further tell about the different parts of the encryption functioning and all the related information with surveillance database .

With enumerating possibilities and regardless of the cultural difference our economy is yet to set out to be an absolutely charged field in each and every way possible.

THE PRIMARY FUNCTION OF DATA ENCRYPTION

The main and the most important function of data encryption is to protect data confidentiality as number of documents are transmitted through various computer devices on a daily basis and in day to day routine. The outdated data encryption standard(DES) has now been replaced by modern encryption algorithms that significantly play a critical role in the protection and security of IT SYSTEMS and COMMUNICATIONS[1]

CHALLENGES TO CONTEMPORARY ENCRYPTION

[1] Data Protection 101,www.digitalguardian.com by Nate Lord accessed 08 May 2020 5:30 pm

The basic method used in today's world is "brute force" i.e. applying various innovative techniques until the right technique simply works. Partly the method of applying a technique depends upon the person who's taking the charge. Alternative methods of breaking a cipher include side-channel attacks and crypto-analysis.

CRYPTO WARS IN INDIA

Despite being a rapidly maturing digital economy, INDIA has not yet experienced and able to gain lightening opportunities of the version of "CRYPTO WARS". However policy developments such as the draft personal data protection bill, the proposed amendments to India's intermediary liability laws indicate and remind us that regulation on encryption based on its perceived hindrance of lawful data collection is imminent[2] .Regardless of other campaigns and strategies India has undergone a tectonic shift in the past few years while delivering specifically targeted schemes launched for the purposes of strengthening the commerce industry and delivering welfare system.

CURRENT ENCRYPTION SCENARIO'S

If we talk about the current take on India or about the present scenario's then it wouldn't be wrong to suggest that it do have restrictions on the sectorial parts such as telecom industries as well as any other plans which may issue general implications. Some examples of such sectorial regulators are the RBI AND SEBI as they mandate minimum encryption standards for entities and transactions acknowledging the key role played by encryption in enabling trust and security

. LAWS OF ENCRYPTION

Sec 84 of the INFORMATION TECHNOLOGY ACT 2000 empowers the government to prescribe modes or methods for encryption by issuing required rules.[3]This was attempted in 2015 when the Ministry of Electronics and IT issued disastrous 'draft encryption policy' which was further withdrawn almost immediately

Sec 69 of the INFORMATION TECHNOLOGY ACT 2000 states the government to issue directions for 'decryption of any information generated ,transmitted, received or stored in any computer resource.[4]

EFFECT OF THE REGULATIONS

The main and the most signified effect of such rules and regulations have been on the private sector, sub optimal information security and roadblocks to innovation. For instance , telecoms are not allowed to deploy 'bulk encryption', the same licence requires them to assure that 'no unauthorized interception takes place(5). Both of these objectives cannot be achieved without a systematic and strong form of encryption policies which could deeply put an emphasis on how to put restrictions on the encryption problems. Highlighting the objectives of government behind mandating weak encryption in telecom sector was presumably to make interception and surveillance easier. While this might have once worked, over the last decade practically all sensitive or

[2] The Encryption Debate in India-William Thomas accessed and retrieved 08 May 2020 5:35 pm

[3] Information and Technology Act 2000,Sec 84

[4] Information and Technology Act 2000,Sec 69

personal communications have moved to heavily encrypted internet applications which are technically resilient and should not subject to the restrictions. Its somehow also unclear that whether India's Intelligence Agencies have really the ability to break currently ubiquitous strong encryption algorithms.

OBLIGATIONS ON INDIVIDUALS TO ASSIST AUTHORITIES

This refers to national legislation or policy which provides for state authorities to be able to require individuals to decrypt of encrypted communications[5]

COUNTRIES WITH OBLIGATIONS ON INDIVIDUALS

AUSTRALIA

Australia comes under the list of top countries in relation to the rules and legislations they generally impose on their individuals. Their authorities and the substantial steps not only protect the rights of their citizens but also record their actions. As per the rules of encryption The provisions of section 3LA of the crimes act 1914 impose the same obligations on individuals as on providers

.

CANADA

No known legislation or policies

UNITED KINGDOM

The provisions of part 3 of the Regulation of Investigatory powers Act 2000 impose the same obligations on individuals as on providers.

UNITED STATES

United States is empowered and socialized with thousands of weapons and resources but it has till now failed to regulate some basic legislations or rules for the encryption terms.

DATA SURVEILLANCE AND MONITORING

People across the world have always been confused between the trade-off security needs and personal privacy including data privacy. Government as a part of such monitoring activities conduct various functions regarding data services and uses the data protection concerns such as surveillance, monitoring etc.

It is very well seen that whenever any terrorist attack happens in our country, people always starts to favour the government about their surveillance programme's that they usually organise through strict functioning of their authorities. But when the same government tries to implement measures for monitoring the activities of these individuals they protest the same government by making harsh comments and by inappropriate use of words through social media platform as well as in daily life activities.

OBJECTIVE OF SURVEILLANCE

The main objective of conducting surveillance is to check on the persons who are suspected through their daily activities of data programming and through social media platform .The main good thing about this surveillance programme is that it doesn't

[5] India's upcoming encryption wars-Factor Daily,factordaily.com accessed 08th may 2020 5:45 pm

discriminate people on the level of caste, colour or religion as for government every other individual who will he against the nation would be termed as criminal regardless of any of his instincts.

DIFFERENCE BETWEEN MONITORING AND SURVEILLANCE

There is no doubt that Monitoring and Surveillance are done to protect the privacy of the people but there's still a lot we're missing here. MONITORING and SURVEILLANCE comes with no. of differences and we really need to throw some light on that.

A simple explanation is that "monitoring" refers to the simple observation of people for commercial purposes but on the other hand "surveillance" comes out with a much wider meaning as it can be defined as a silent act of monitoring and collecting important and crucial data from the device of a suspected person.[6] Surveillance is mainly done by the Government for security reasons and ensuring that the statehood policies and its dignity is not in danger and the country is safe throughout.

STEPS FOR SURVEILLANCE

Some recent steps have been taken by the authorities with a view to improvise the policies of its department in relation to SURVEILLANCE PROGRAMMES . On 07.Nov.2019 ."Facial Recognition System" has been introduced by the authorities for easy catching of the one's who are suspected by the police department.

FRS is basically a camera based technology which is implemented at different public places so as to record their actions and catch the suspect lively through his actions and intentions both. It is a technology capable of identifying or verifying a person from a digital image or a video frame.

FACEBOOK DEEPFACE

Living in a modern era with social websites generating their wheels to success leading paths .it is always recommendable to watch the actions of these social networking sites by the crime investigation cells and see that if they are not doing any inappropriate activity with the data of public. Now recently Facebook's Deep Face has become the subject of deep concern. Several active class lawsuits has charged up and taken up their responsibilities under the Biometric Information Privacy Act, with claims alleging that Facebook is collecting and storing face recognition data of its users without obtaining informed consent from them, it is a direct violation of the Biometric Information Privacy Act the most recent case was dismissed in January 2016 because the court lacked jurisdiction in it[7] .Therefore it is still unclear if the Biometric Information Privacy Act will be effective in protecting biometric data privacy rights. In December 2017,Facebook rolled out a new feature which indicates that when any of your friend uploads and tags you in a photo FACEBOOK will automatically tag you according to your face instincts or we can say features without taking your prior consent for it. This new feature not only violates right to privacy but it will also give birth to number of hindrances coming in future. Facebook has attempted to frame new functionality in a positive light,

[6] Data Surveillance, Monitoring and Spying by Cathy Nolan accessed and retrieved 09th may 2020 10:30 pm

[7] 'Facebook keep getting sued over Face Recognition Software'-International Business Times

amidst prior backlashes.[8]it is still contested as to whether or not facial recognition technology works less accurately on people based on their competitiveness.[9]Experts fear this very new technology might have a bad impact in the lives of people but police is protecting the claims by saying that FRS is implemented for the security reasons and not for any other undesirable reasons or basis.

The lack of regulations holding facial recognition technology companies to requirements of racially biased testing can be a significant flaw in the adoption of use in law enforcement.

COVID-19 and SURVEILLANCE

We all are well aware of the Corona outbreak in the country and the level of problem and frustation that we all are dealing with .The situations are even worst in the much developed countries such as Italy, Spain And US . But the problems and frustation level of the people who are stucked in their homes are not ought to be finished yet and as a result they are coming out of their homes to resemble again and carry on their day to day works. Summarising all this the main problems for the people who are engaged in restricting them in their homes are increasing as the people are not yet becoming responsible for their acts .For this the main and the most crucial role played by the intelligence beaureu is by the FRS system as they are already having an eye on the people who are not ready to sacrifice their cultural as well as moral beliefs for their own lives. As a result intelligence beaureu and other authoritative responsible committee's have taken a step to charge the offenders with procured punishment and to put necessary restrictions. Corona has not only increased the tensions of the individuals but has also affected and increased the burden on the investigating authorities as for them the workload is now more emphasised by the government.

CONCLUSION

By this research paper the conclusion that came out to be is every other thing on this planet has somehow affected the social, technical and linguistic backgrounds of the devastating economy of India. Data encryption and surveillance tools are necessary for the well working systems of social networking as well as for data protection purposes but at the same time "Private Privacy" should also be taken into consideration and maximum efforts should be made that if intelligence terminals have made their mind to put surveillance on any individual's data then in that case they must take measures to protect that person's data from any non authoritative person.

*****

[8] 'Hera Dana Judge tosses illinois privacy law vs Facebook over phototagging,Cookcountryrecord.com accessed and retrieved 09th May 2020 10:45 PM

[9] 'Facebook can now find your face even when it's not tagged'-TIMES NOW published and accessed 09th may 2020 11:05 PM