VOLUME 4 ISSN 2456-9704

ARE WE READY? – PRIVACY, DATA PROTECTION AND GOVERNANCE

By *Damini Krishan*
From *University of Mumbai Law Academy, Mumbai*

INTRODUCTION

"India has physical boundaries in terms of its geographic location with other countries, but there was no such 'boundary' in the cyber world. "Our cyber boundary is not (yet) defined. We have to protect our cyber boundaries also.[1]

In Modern Cyber World, computers and internet have become a vital part of human life. They have been invented to make human life easy, but when you take each and every micro step towards making your life easy, the internet asks you to give away some part of your individual privacy. So, now the main question arising here is, whether people are ready to give away some part of their privacy directly or indirectly on internet platforms and associated persons and organizations? The best example of above-mentioned situations would be giant companies like Facebook, Twitter, Instagram, true-caller, and other organization which always seek some sort of confidential information from the concerned users upon accessing their websites, like true-caller always asks the concerned users to access their phone contacts, messages, etc.

In United Kingdom (UK), Minister of state for Digital, Culture, Media & Sports (DCMS) spoke about the new Data Protection Law (DPL) which would include the concept of 'Right to Forgotten' by companies. [2] Thus, these giant corporates would no longer be able to reuse people's data submitted and consented by people for their one-time service. The said bill also expanded the ambit of "Personal Data" to include IP address, internet cookies, and DNA. The Legislature of UK will also give the power to Information Commissioner's Office to impose fines of up to 17 million Euros or 4% of the global turnover of the concerned entity along with criminal liability, for breach of the new DPL. This law envisages to meet the parameters of this contemporary cyber world so that interest of citizens can be protected by not endangering their privacy.

FACEBOOK TERMS AND CONDITIONS

In the ***"Statement of rights and responsibilities"*** of Facebook, clause 2 (1) says that

"For content that is covered by intellectual property rights, like photos and videos (IP content), you specifically give us the following permission, subject to your

[1] India yet to sign treaty with other countries on Cybercrime, says CBI special Judge the Hindu, http://www.thehindu.com/sci-tech/technology/internet/India-yet-to-sign-treaty-with-other-countries-on-Cyber-crime-says-CBI-special-Judge/article12546205.ece

[2] Gov.uk. (2017).Government to strengthen UK data protection law - GOV.UK. [online] Available at: https://www.gov.uk/government/news/government-to-strengthen-uk-data-protection-law

privacy and application settings: you grant us a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP content that you post on or in connection with Facebook (IP License). This IP License ends when the concerned user deletes his IP content or his account unless his content has been shared with others, and they have not deleted it."

It is well-known fact that Facebook is the biggest player in the field of social networking and it uses third party applications and has partnerships with other global companies. Clause 2(1) gives a right to Facebook to use content uploaded by users on its platform in a manner as it deems to be fit. Further, it extends authority to Facebook to transfer user's data to any other organization as it considers appropriate.
If the user wishes to delete any content from Facebook, first the user would have to delete that content from his/her account and if the user has tagged someone then that concerned user also has to delete that content.

PRIVACY AN EMERGING CONCEPT IN INDIA WITH RESPECT TO UK, USA AND EUROPE

Privacy was nowhere in the "news" withrespect to India until the Aadhar Incident happened where thousands of cases emerged in relation to the leaking of sensitive information containing the biometrics of people. This incident has led to a 360-degree change in mindset of Indian citizen and now people are questioning the government about the security of their personal information with the government considering recent incidents like "Wanna Cry ransomware" which has already led to a lot of chaos in developed countries like UK, US, etc. by putting at stake the confidential information of the citizens of this country.
India being a developing country is taking giant strides towards economic prosperity and growth which is being acknowledged by many of the developed countries. However, India still lags behind in relation to cybersecurity and data protection in comparison to the more technologically advanced countries of the world. A total 50 incidents of cyber-attacks affecting 19 financial organizations have been reported from November 2016 to June 2017 as stated by the Government of India.[3] These attacks have been reported majorly on Payment gateway or digital payment interfaces that include e-wallets like Paytm, Jio-Money, etc. and these incidents have only been reported in relation to the financial sector. Many unreported incidents have also taken place in other sectors as well which haven't yet come in front of the public eye.A report by India.com mentions that 'a total of 1.71 lakh cyber-crimes were reported in India in the last three and half years. This means at least one cyber-attack was reported every 10 minutes in initial six months of 2017.[4]

Reported by The Economic Times on 15 MAR, 2012, 05.15AM IST, ET BUREAU *"About 112 government websites, including*

[3] Total of 50 cyber-attack incidents reported in financial sector: Govt The Indian Express, http://indianexpress.com/article/technology/tech-news-technology/50-cyber-attack-incidents-reported-in-financial-sector-govt-4777350/

[4] One cybercrime in India every 10 minutes - Times of India The Times of India, https://timesofindia.indiatimes.com/india/one-cybercrime-in-india-every-10-minutes/articleshow/59707605.cms

those of Bharat Sanchar Nigam Ltd, Planning Commission and Ministry of Finance, were hacked in the last three months, minister of state for communications and IT Sachin Pilot said in the Lok Sabha"[5]

There is technology to obtain a person's fingerprint, say from a book he/she is reading or from high-resolution images posted on the social media platform. In 2014, for instance, hacker Jan Krissler recreated the fingerprints of Germany's defense Minister Ursula von der Leyen from close-up photographs in a government press release. [6] Advances in technology means stolen prints can be used to make the three-dimensional facsimile.

Keeping all these attacks in mind our beloved PM has prepared an Information aquarium in which Biometrics and other confidential data of the citizens are stored. This information aquarium is also online with high cybersecurity. The question here is not why the government is collecting our personal data, however. the question here is how secure is that Information Aquarium when cyber-attack like "Wanna Cry ransomware" have already breached the security level of the Indian government.

In respect of new cyber-attack that happened in 2017 like "Wanna Cry ransomware" which almost netted 52 bitcoins or about 130000$. Shadow Breakers is another infamous name in the domain of cybersecurity, this mysterious group 1st launched its identity in August 2016 claiming to have breached the spy tools of the elite NASA-Linked operation known as the Equation Group. Further, they also offered a sample of stolen data of NASA.[7]
On March 7 "WikiLeaks CIA Vault 7" another mysterious hacker group which published 8,761 trove documents allegedly stolen from the CIA that contains hacking tools. Revelation included iOS and Android vulnerabilities, bugs in windows, and the ability to turn some smart TVs into listening devices.[8]

Acknowledging the above mentioned incidents and to ensure the protection of its citizen's data, United Kingdom (UK) has decided to overrule its previous data protection law [9] i.e. Data Protection Act, 1998 by passing new Data protection law in 2018 this bill will include a high level of fine for breach of any data and also give the"Right to forgotten" to the citizens of UK.
Information and Technological Act 2000 [10] hereafter referred to as (IT Act) provides

[5] 112 government websites hacked in 3 months: Sachin Pilot The Economic Times, https://economictimes.indiatimes.com/tech/internet/112-government-websites-hacked-in-3-months-sachin-pilot/articleshow/12270733.cms

[6] Fingerprint 'cloned from photos', BBC News (2017), http://www.bbc.com/news/technology-30623611

[7] Andy Greenberg et al., Hackers Claim to Auction Data They Stole From NSA-Linked Spies WIRED (2017), https://www.wired.com/2016/08/hackers-claim-auction-data-stolen-nsa-linked-spies/

[8] Lily Newman et al., The Biggest Cybersecurity Disasters of 2017 So Far WIRED (2017), https://www.wired.com/story/2017-biggest-hacks-so-far/

[9] UK data protection laws to be overhauled, BBC News (2017), http://www.bbc.co.uk/news/technology-40826062

[10] Dot.gov.in (2017), http://www.dot.gov.in/sites/default/files/itbill2000_0.pdf

some sort of relief to Indian citizens. This act, however, does not provide proper armor to the Indian citizen to defend them self from the hackers who are sitting outside the territorial jurisdiction of India. The main question that arises here is that, how would this act punish a criminal who is operating beyond the limits of India's territorial jurisdiction and the IT Act?

In spite of having IT Act Aadhaar informations were leaked and one of the best examples of this would be **Suvidhaa-Axis Bank Case***on February 11, a YouTube clip illustrating such a replay attack was divulged online. On February 24, UIDAI lodged a criminal complaint, contending that an employee of SuvidhaaInfoserve had used Axis Bank's gateway to UIDAI's servers to conduct 397 biometric transactions between July 2016 and February 2017 using a stored fingerprint. Axis Bank representatives did not respond to requests for comment.*

One of the solution to tackle this type of situation is Bilateral extradition treaty with other countries. Till now India is only part of 42 Bilateral extradition treaty out of 195 countries in the world. [11] India has Extradition Arrangements with 9 countries including Sweden, Italy, etc. The Extradition Arrangements with Italy and Croatia confine to Crimes related to Illicit Traffic in Narcotics Drugs and Psychotropic Substances owing to the fact that India, Italy, and Croatia are parties to the 1988 UN Convention against Illicit Traffic in Narcotics Drugs and Psychotropic Substances.[12]

AN ANALOGY BETWEEN THE LAWS OF UK, US, EU & INDIA

Creating an analogy and comparison between the laws of developed countries like the UK, EU, and India, gives a vivid picture of Indian scenario that Indian legislature needs to acknowledge that India needs a Data Protection Act to maintain the law and order in this contemporary world. We all can acknowledge that UK has its Data Protection Act of 1998 which is solely designed for the protection of privacy and data of the UK citizens. Furthermore it is announced by the UK Minister for state for Digital, Culture, Media & Sports (DCMS) to overruled it previous Data Protection Act to cop up with the requirement of this contemporary world.

According to the UK Data Protection Act of 1998, the people and Organizations tangled in storing personal data shall have to register with the information commissioner, who is appointed by the government as an officer of the government in order to keep a check and balance on the rules and regulations adopted by the Act. The Act provides a certain restriction in the gathering of personal and sensitive information. Any personal data or information can be demanded only for one or more lawful purposes and the same data or information cannot be further processed or used for multiple purposes apart from the task/tasks that it was required for. The personal data should not be excessive and the data or information which is being demanded should be relevant and correct and adequate for the purpose(s) it is needed and to be processed. It is quite appreciable

[11] MEA | List of Extradition Treaties/Arrangements, Mea.gov.in (2017), http://www.mea.gov.in/leta.htm

[12] id

and indispensable fact that UK, US, EU are trying to enhance their Data Protection Act so that no criminal can abscond from the law and justice can be delivered.

The US has quite a different approach when it comes to Data Protection of its citizen. They follow the sectorial approach in which sensitive data of their citizen are grouped in classes on the basis of their utility in the US, thus they have a concept of the mixed legislature when it comes to Data Protection. EU has its own Data Protection Act which is quite advance and have the capability to cope up with the requirements of this contemporary world. European Union Data Protection Act (hereafter referred as EUDPA) is applicable on all countries who are the member of EU, further it is applicable on those company or countries who want to trade with EU. Hence it is indispensable fact that if India wants to do trade with EU then India needs to comply with the laws of EU. Recently EU official has published a list of adequate countries which includes **Andorra, Argentina, Canada (commercial organizations), Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, and Uruguay** but India still needs to work on its Data Protection laws to get enrolled in EU list.[13] EUDPA says that "*Personal data shall not be transferred to a country or territory outside the EEA unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.*"[14]

So, it is quite vivid that EU has some sort of set standards which has to meet if any data has to transfer to countries outside the European Economic Area (hereafter referred as EEA).

India has only one law which partly serves some sort of data protection but India legislature should acknowledge the fact that IT act is not sufficient to deliver justice in this cyber advanced world. India needs a comprehensive and complete data protection act so that no criminal can abscond from the law and justice can be delivered.

The IT Act, 2000 is a general Act which has its main focusses on crimes like the digital signatures, cyber contraventions and offenses, e-governance, confidentiality. It is mistaken and is erroneously compared to the European Directive on Data Protection (EC/95/46), OECD Guidelines on the protection of Privacy and Transborder Flows of Personal Data and the Safe Harbour Approach of the US.

The fact is that the IT Act, 2000 deals with the issue of the Data Protection and privacy in a partial manner. There is a lack of actual framework in the IT Act, 2000 wherein the Data Protection Authority and quality and transparency of the data are considered. Even if the legislature of India tries to amend the IT Act, 2000 then also there would be some loop-holes for the actual

[13] Commission decisions on the adequacy of the protection of personal data in third countries - European Commission, Ec.europa.EU (2017), http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm

[14] Sending personal data outside the European Economic Area (Principle 8), Ico.org.uk (2017), https://ico.org.uk/for-organisations/guide-to-data-protection/principle-8-international/

framework and guidelines for data protection and privacy that should match the EU directive, OECD Guidelines or the Safe Harbour Principles.

Because of the absence of Data Protection Laws, India is ona heavy loss to the outsourcing industry. Though it is a flourishing industry in India but we do not have a proper Data Protection Act. The customers in the US and the European Union are protected by the comprehensive privacy directive which focuses on the principle that the personal data should not be transferred to countries which do not have adequate protection policy. As a result, for European trade Union data protection is an indispensablerequirement which has to be acknowledged in these international out-sourcing companies. Hence this may lead to a slab in the outsourcing industry in India. Hence India needs to tackle this situation tactfully and should consider the importance of Data Protection Act.

CONCLUSION

In this contemporary cyber world, we have to acknowledge the fact that India is still lagging behind from European countries in terms of cyber laws and it's not a fortnight job to introduce a new cyber law in India. India is a growing economy where lots of data is transferred from India and there is an urgency of law and legal framework to monitor this data before it is too late for this booming economy. In this cyber world not to have an adequate Data Protection Act becomes a slab and this prevents India to become one of the developed cyber economies.

Till now there is no significant research has been done in respect of trans-border data flows. Indian legislature should be proactive and have to divert its concern on the urgency of law and legal framework required in this field. We all know India is a developing country one of the benefits of being developing nation is they don't have to start from zero. India can take into the consideration different laws and model of developed countries which already have stable Data Protection Act like UK and EU. Till now the only act which deals with some sort of data protection in India is IT act but IT act is a general act and it is sometimes not able to punish the criminal because of loop holes in the act. So, before it becomes too late, India should introduce its new law for Data Protection so that in future no criminal can abscond from the law and justice can be delivered.

REFERENCES

1. India yet to sign treaty with other countries on Cybercrime, says CBI special Judge the Hindu, http://www.thehindu.com/sci-tech/technology/internet/India-yet-to-sign-treaty-with-other-countries-on-Cyber-crime-says-CBI-special-Judge/article12546205.ece

2. Gov.uk. (2017). Government to strengthen UK data protection law - GOV.UK. [online] Available at: https://www.gov.uk/government/news/government-to-strengthen-uk-data-protection-law

3. Total of 50 cyber-attack incidents reported in financial sector: Govt The Indian Express, http://indianexpress.com/article/technology/tech-news-technology/50-cyber-attack-incidents-reported-in-financial-sector-govt-4777350/

4. One cybercrime in India every 10 minutes - Times of India The Times of India, https://timesofindia.indiatimes.com/india/one-cybercrime-in-india-every-10-minutes/articleshow/59707605.cms

5. 112 government websites hacked in 3 months: Sachin Pilot The Economic Times, https://economictimes.indiatimes.com/tech/internet/112-government-websites-hacked-in-3-months-sachin-pilot/articleshow/12270733.cms

6. Fingerprint 'cloned from photos', BBC News (2017), http://www.bbc.com/news/technology-30623611

7. Andy Greenberg et al., Hackers Claim to Auction Data They Stole From NSA-Linked Spies WIRED (2017), https://www.wired.com/2016/08/hackers-claim-auction-data-stolen-nsa-linked-spies/

8. Lily Newman et al., The Biggest Cybersecurity Disasters of 2017 So Far WIRED (2017), https://www.wired.com/story/2017-biggest-hacks-so-far/

9. UK data protection laws to be overhauled, BBC News (2017), http://www.bbc.co.uk/news/technology-40826062

10. Dot.gov.in (2017), http://www.dot.gov.in/sites/default/files/itbill2000_0.pdf

11. MEA | List of Extradition Treaties/Arrangements, Mea.gov.in (2017), http://www.mea.gov.in/leta.htm

12. Commission decisions on the adequacy of the protection of personal data in third countries - European Commission, Ec.europa.EU (2017), http://ec.europa.eu/justice/data-protection/international transfers/adequacy/index_en.htm.

13. Sending personal data outside the European Economic Area (Principle 8), Ico.org.uk (2017), https://ico.org.uk/for-organisations/guide-to-data-protection/principle-8-international/.

*****