Conundrum Of The Advances And Restrictions Of Digital Rights And Face Recognition

[1]Suresh Kumar Gigoo, [2]Beena Gigoo
[1]Director(Operations and Stategy), [2]Educationist/Academician
Gigoo Omni Quality Enterprises

Abstract - **In an increasingly Internet penetrated world, helped now, by the imminent rolling out of 5G technologies and faster fibre lines ,even in underdeveloped countries, the power of information and always-on connections on web through many channels has truly democratised the world. The boundaries of developed and developing world are vanishing by the day with some great and innovative work in digital enablement and payments emerging from such countries like Kenya, India, Indonesia, South Africa and other countries. The new paradigm of social media has played a significant role in improving the lives of citizens and disadvantaged. The MeToo movement, swift mobilisation/help during disasters/floods and recent Covid-19 pandemic has unlocked the potential of social media in many ways. However, some elements have also piggybacked or misused the social media for ulterior motives/nefarious ends. The present world is a paradox. While the need for digital rights is getting ever stronger by the day, with several curbs/filters maturing in traditional geographies like Europe, paradoxically the world is getting ever open/transparent with ubiquitous power of CCTVs and now Face Recognition, biometrics, Artificial Intelligence playing role in increasing transparency/openness but with attendant truncation in privacy. But, in today's world already digital adoption is a fact of life. The debate between privacy and transparency notwithstanding, the world will increasingly be more open and less private. Facebook is a good case study where face recognition has been increasingly adopted and accepted by customers. The paper will examine the evolving scenario of digital rights and the paradox of adoption of new generation invasion of such technologies like face recognition, artificial intelligence etc.**

keywords - **Digital Rights, GDPR, Digital Privacy, Digital Transparency and Security, Artificial Intelligence, Face Recognition, Facebook**

Introduction

The present world has been described by many theorists, thinkers and strategists as VUCA World where all aspects are constantly and predictably volatile, uncertain, complex and ambiguous. Mankind's evolution has witnessed several events over the millennia where it has been necessary to march in lockstep with the evolving technological changes. The changes may have disrupted the social, sociological and humanist aspects in a benign way as well as harsh way on many occasions. But, evolution perhaps has no respect or magic wand to control, stall and manage events. Evolution has no timetable or plan .It moves to the rhythm of time and space without the certainty and prediction of an early morning sunrise or evening sunset.

Mankind is evolving in the giant time machine on a continuous basis. Based on the tremendous turmoil of the first half of the 20th century when mankind faced brutal global level wars, a need was felt to secure/protect/defend the common humanity around the globe in a formal, legal way. This resulted into declaration of Universal Declaration of Human Rights by the Unites Nations General Assembly on 10 December 1948.The document was precipitated by the excesses of the world wars, but the document was in a way waiting to happen also as a result of anger, humiliation and exploitation in many parts of the world by events like Industrial Revolution, colonialism, trade exploitation, religious persecution, human trafficking and the snobbery from emerging weapons. For a while, it had appeared that humans in humans had taken a back seat.

Till this game changing document arrived. The world is never the same. The document in many articles covers the requirements and compliances. With the democratisation of the world in cyberspace (in physical world time may have to wait bit longer perhaps),the human rights aspect has now got extended to a new wave of rights. These are the digital rights. With the ever deepening of Internet penetration and mobile penetration and especially due to social media giants like Facebook, Twitter, Instagram and Internet giants like Google in all aspects of human lives across the globe in 21st century, there has been a crying need necessitated for digital rights of citizens.

At the same time, the requirements and difficulties of governments in maintaining healthy law and order in cities and villages must not be underestimated. There should not be free for all situations under the garb of freedom of expression. Templates of developed countries may not be possible to replicate at all places. Bias of manipulation, fiendish designs of evil forces and disgruntled elements must not be disregarded in this regard.

The New Vulnerabilities and looming dangers in Cyberspace

In an article in Bengaluru based daily Deccan herald on 16 December 2019[1], it was reported that data breaches had cost Indian companies around Rs. 12.8 crore from July 2018 to April 2019 based on IBM data. The famous data breaches brought out the poor defences and cyber protection in a number of cases. These are:-

a) Aadhar Data leaks in Andhra Pradesh and Jharkhand.
b) Attack by a purported North Korean malware on India's famous nuclear reactor at Kundankulam, Tamil Nadu.

c) Spying incident of Israeli Pegasus software on Indian journalists/activists.
d) 419 million accounts of Facebook faced data leak

As a result, the new frontiers for defending are not only limited to physical borders alone. The new cyberspace threats are a clear and present danger. There is a new requirement to have Digital Rights for Digital Protection and protection from digital invasions and digital intrusions. When big, organised entities are facing cyber threats and breaches, small entities and humble cyber customers and individuals need more defences and cyber rights. The present Internet has issues including rampant abuse, hate speech, censorship, bias, and disinformation. Search engines, social media platforms, and infrastructure providers have huge influence on what we are allowed to see and say[2] .

Privacy today for consumers has to be built by tools of better rules and designs inbuilt in systems. The present regime of exploitation may not be tenable.[3] The digital world has today opened the doors to surveillance capitalists to exploit the data collected from customers as brilliantly argued in seminal work.[4]

Hereon, we will analyse various aspects of Digital Rights in following paragraphs now.

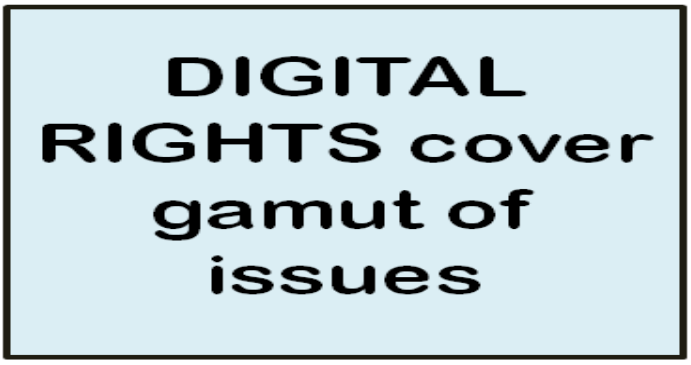

Fig. 1 Digital Rights have increased in scope with evolution in technology

Digital Adoption-still work in progress

While on a daily basis we hear the growth of telecom and Internet providers, it is still work in progress in many ways. The data below shows that there is still a lot to do in many ways to make the world fully online/digital/cyber ready for many aspects including E-Commerce. As far as countries who have adopted digital platforms, the digital aspects will be the next level of work to do. On a day to day and continuous basis.

Serial No.	Category	Percentage of countries adopted
1.	Countries with E-Transaction laws	79 %
2.	Countries with Consumer Protection Laws	52 %
3.	Countries with Privacy laws	58 %
4.	Countries with Cybercrime Laws	72 %

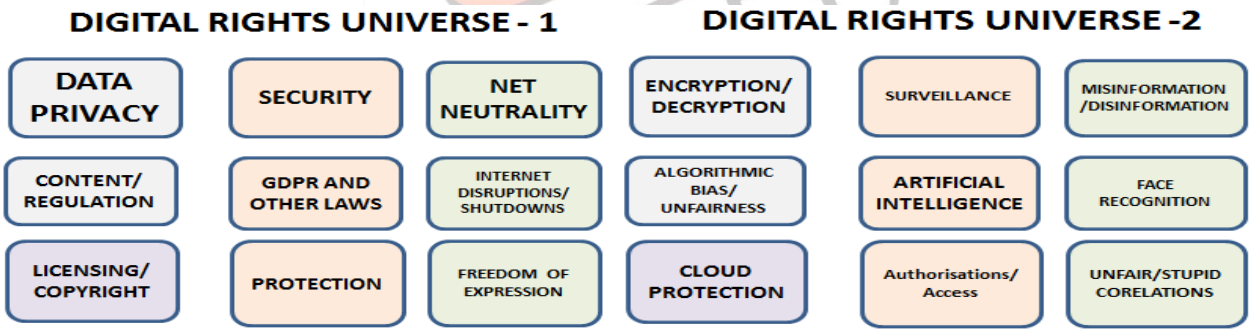

Fig. 2 Adoption/legislation Status of E- Commerce in 194 countries (Source: UNCTAD, 14 Jan 2020)
Fig. 3 In today's Internet penetrated world, Digital Rights cover a gamut of issues

Path breaking Laws/Statutes related to Digital Rights/Privacy

Several types of laws and statutes are active/in vogue in various countries. While majority of them are focussed on Data protection and privacy, some of them are also being used by governments e.g. Singapore to thwart any disinformation/fake news/panic spreading and enable correction issuance feature. While some have criticised this feature, but from government's point of view it is very helpful to maintain civic peace and order and not have street chaos as is now happening increasingly in many geographies of the world.

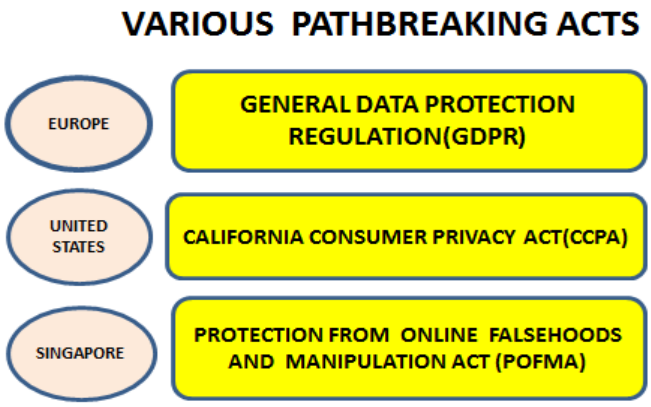

Fig. 4 Spectrum of digital privacy laws include many facets across the globe

EU's GDPR

Replacing the previous version of Data protection document, the EU's brought out a path breaking promulgation in the form of General Data Protection Regulation[5] (or GDPR) . As of now, the document addresses the needs of privacy and protection of the consumers/citizens/common people in many ways. But in the cat and mouse game of protection and new technology trends, time to time various revisions/modifications/amendments/supplements may be necessary. The future proofing of the GDPR Directives may not be 100 per cent possible but there has to be will at all levels to enable the same. Common man/organisation is the centre of attention as regards privacy and protection is concerned in this document.

Fig. 5 Pathbreaking GDPR is inspiring many other countries in the world(Image credit as per Bibliography)

The document consists of 99 Articles. Each and every Article is a must study and educates and informs us the necessity of adherence. Brazil from BRICS group of countries is switching to LGPD inspired by GDPR from February 2020.

Salient features of GDPR are described below:-

a) A common harmonised umbrella of data protection law from the previous 28 different laws under Data Protection Directive 95/46/EC(DPD).
b) Requires respective Data Protection authorities in all EU countries.
c) Requires designation /nomination of Data Protection Officer (DPO) akin to Management Representative (MR) as was required for ISO 9001:2008 QMS standard for organisations as contact point for all Data Protection related matters.

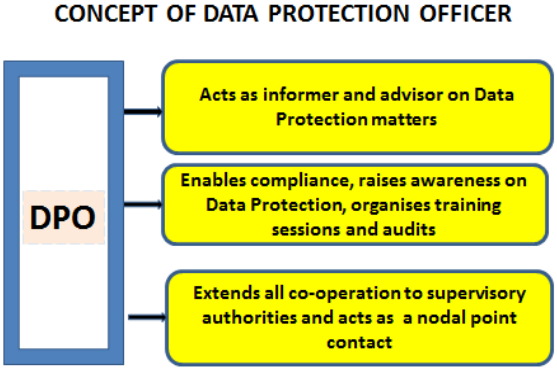

Fig. 6 Data Protection Officer Concept is a very good feature of GDPR

d) Adopted on 14 April 2016, but, effective from 25 May 2018
e) Right to erasure or Right to be forgotten of a personal data concerning data subject without undue delay.
f) Right to Access personal data processed with purposes of processing, categorizing of data.
g) Philosophy of Privacy by design is incorporated.
h) Right to be informed feature for users develops culture of transparency and protection.
i) Encryption feature for better protection of data for individuals is strongly advocated by the Regulation. This extends to using pseudonymisation[6] and obfuscation/tokenisation[7] of data to prevent third parties to know the data. This builds up huge protection and privacy.

j) In order that companies are discouraged/ dissuaded from noncompliance to GDPR Regulations, a strong Fines/penalties Article can be invoked. As per GDPR Enforcement Tracker[8], already almost 190 companies have faced the penalties including big names like Google.

Fig. 7 GDPR has already punished many entities including Internet giant Google for non-compliances and violations

EU's NIS Directive(2016/1148)

In addition to GDPR as mentioned above, EU NIS Directive[9] is focussed on providing commonality of Network and Information systems across the EU. This is targeted for provider of mostly essential services like energy, water, financial infrastructure, banking and healthcare. Leveraging this, the cyber security improves for:-

- Online marketplace
- Online search engines
- Cloud Computing services

America's CCPA

Though being home to famous Silicon Valley and Internet giants and many innovative startups, Americans had less privacy/protection laws previously. But with the leadership mantle of protection/privacy donned by EU through GDPR, some states in America are now waking up to the need for privacy. Therefore, a landmark legislation[10] of California Consumer Privacy Act(CCPA) was enacted in 2018.The same is effective from 01 January 2018.Salient features of the Act are:-

- Rights of consumers include:-
  a) Right to know.
  b) Right to delete
  c) Right to opt out
  d) Right to non-discrimination

Fig. 8 CCPA is a first of its type law in the land of internet giants(Image credit as per Bibliography)

- Applies to businesses having gross annual revenue of more than USD 25 million and other criteria related to number of customers
- Personal information defined more broadly to include identifiers (like name, alias, SSN number, telephone number, medical insurance number ,biometric information, IP address, email etc.)
- Act is applicable to businesses, service providers and third parties
- Forbids any retaliatory actions against consumers for exercising respective rights under the Act

ISO 27701

On the lines of ISO Standards like ISO 9000 series, a new Standard[11] ISO/IEC 27701:2019(E) exclusively devoted to Information Security Management aspects has been published. The Standard specifies the requirements for establishing, implementing, maintaining and continually improving a Privacy Information Security Management system within the context of the organization. It is an extension of ISO/IEC 27001 and ISO/IEC 27002.Salient features of the ISO Standard are shown in infographic below:-

Fig. 9 Recently formulated ISO 27701 Standard has various aspects for better privacy

Social Media Privacy Protection and Consumer Rights Act of 2019

This law was introduced in US Congress on 17 January 2019 and has been referred to a Committee[12]. The stated objective of the law is "to protect the privacy of users of social media and other online platforms." The important salient features include:-

a) Prior to a user creating an account online, the Online platform operators must intimate users that his/her data produced during online behaviour will be collected and used by the operator and third parties.
b) Onus on operator to establish and maintain privacy/security program for online platform and publish its description .
c) Disclosure aspect in that operator must disclose to users the terms of service for usage of online facility including the collection and use of personal data in accessible form,non lengthy form and clearly distinguishable in cogent and clear language.
d) On introduction of new products/changes to privacy or security programs,operator to pre-inform users
e) Ease of withdrawal of consent clause.
f) 72 Hours time limit ,this is the time within which operator must notify users in the event of occurrence of transmission in violation of privacy/security program.
g) Deviation or violation in contravention to the bill's privacy requirements will be considered an unfair or deceptive act or practice under the Federal Trade Commission Act

Other Noteworthy Laws

Several other laws also offer protection to various degrees in the US. Some of these are:-

a) Fair Credit Reporting Act(FCRA),1970
b) Video Privacy Protection Act,1988
c) Graham Leach Bliley Act,1999
d) Cable Communications Policy Act,1984
e) Electronics Communications Privacy Act,1986
f) Health Insurance Portability and Accessibility Act,

Trends in India – The Personal Data Protection Bill, 2019

India, even though an IT superpower, is planning to have its data protection regime in place only now with the Bill [13] recently introduced in Parliament. The stated purposes are**:-**

- to provide for protection of the privacy of individuals relating to their personal data, specify the flow and usage of personal data
- create a relationship of trust between persons and entities processing the personal data,
- protect the rights of individuals whose personal data are processed,
- create a framework for organisational and technical measures in processing of data
- laying down norms for social media intermediary
- cross-border transfer, accountability of entities processing personal data remedies for unauthorised and harmful processing,
- Establish a Data Protection Authority of India for the said purposes and for matters connected therewith or incidental thereto.

Singapore – The trend of General Correction Directions under POFMA and arresting the falsehoods online

In October 2019,Singapore promulgated[14] Protection from Online Falsehoods and Manipulation Act (POFMA) to rid the country of growing menace of fake news spreading and wrong reporting. The directives under this law includes steps like :

- Correction: In case the information on social platforms has been found false, individual/entity is required to publish that same is false.
- Stop communication: Stoppage of communicating the false statement is mandatory.

- Targetted correction: Internet platforms have to clarify to their Singapore end-users that the offending statement, or part of it, is false. They will also have to give a specified statement of fact, or point out where the specified statement can be found.
- Disabling: Internet platforms must disable access by Singapore end-users to the false material.
- General correction: Any time some wrong/fake/malicious content is promulgated on Internet platforms ,ISPs and media organisations have to communicate, publish, broadcast or transmit a correction notice to their end-users in Singapore.
- Account restriction: Fake online accounts, such as bots must be restricted by ISPs from using their services or interacting with their other end-users in Singapore.

The authorities have found this tool handy to control spread of rumours and panic during the Coronavirus spread period in recent times[15].

Growing Global Internet Shutdowns

Though some sections have criticised the provisions of the laws citing intrusion of data privacy, but from Government's sensible point of view decision appears correct. In today's world, people are coming to streets more often than in previous times as more accessibility and spreading the word/message is possible due to democratisation of communications and Internet. In recent times ,across the world people have come to streets in places as varied and apart as Chile,Lebanon,France,Hong Kong,India,Algeria,Chad,UK,Zimbabwe ,Peru etc. In digital world, ironically streets are getting more flooded with people than in non-digital world. This is a worrisome aspect. The existential dilemma whether to regulate [16]online content has been discussed. Putting undue pressures on governments ,manipulated or otherwise, will create crisis of its own e.g rising populism, bad fiscal discipline and lost business and lost credit ratings. But governments will have to find out some other ways than to go for Internet shutdowns. Several parts of the globe have been afflicted by the shutdowns [17] in Chad[18] ,Liberia[19],India[20].That is like a lazy solution.

The Era of self-regulation yields to new world of oversight by authorities

Internet giants like Google, Facebook and Twitter have had a field day till now. Their self-regulation of the content has been initially loose, evolved towards moderate responsibility; yet, it is a far cry of a better/responsible stakeholder devoted to improve humanity fairly. This world is theoretically free everywhere, but there are bounds and restrictions to live in any place. Fortunately, in a terrorism and war ridden world it is becoming clear that oversight on the social sites is inevitable. As cyberspace becomes more spread out, the empires of governments are also catching up to ensure incident free governance in their respective lands. In this regard, good old EU is again taking a lead.[21] The discussion is underway to fine entities if any terror/terror provoking content is on social media sites for more than one hour. Australia which watched helplessly the streamed terror unfold in nearby New Zealand has learnt a lesson and taken recourse to new law[22] by promulgating Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019.This law has various provisions to punish hosting entities in the cases of using abhorrent violent conduct. eSafety Commissioners, nominated on the provisions of Enhancing Online Safety Act,1995 have been given vast powers under the new Act. Abhorrent violent conduct gets committed in following cases:-

a) engages in a terrorist act; or
b) murders another person; or
c) attempts to murder another person; or
d) tortures another person; or
e) rapes another person; or
f) kidnaps another person

India is also waking up to the challenges caused by mass disruptions, street protests and in many cases misuse of social media. Government is also not taking any chances. Ratcheted up by the recent events of circulation of fake news , Narendra Modi Government has now indicated about a plan to regulate[23] social media.

The idea of Panel of Friends for Good Net Oversight/Access Control

Across the world, there is a tendency that governments are acting like "big brothers", overly poking/intrusive authority, unnecessary needling authority. However, the role of the government is like a father, at once caring but also strict and vigilant. But governments these days need not take direct flak/controversy. Today's governments must learn to outsource "dirty work" to various entities after those meet some basic Qualitative requirements/conditions. Today's social media can be better monitored in the following proposed way:-

a) On the style of Friends and Friends of Friends,Facebook can be persuaded to also have a rotating(not permanent) panel of "Good/centred/balanced" people representing a cross section of society in more democratic manner .Keeping repetitive same members like IT bigwigs/industry bigwigs/political bigwigs may not be helpful. Panel should comprise of young and old, representatives from sports/music/films/education/engineers/doctors/etc. Let us call them the Big Friends Panel.
b) The panel may be local geographical, regional geographical, national geographical and in international matters international geographical. A UN like body for cyberspace will be able to bring more order to the unregulated chaos. Templates from IATA, UNESCO,WHO (not Security Council) may be helpful.
c) Facebook may be encouraged to keep these panels in the customers friends list at all times. The Panel will have following rights:-
    - Poking Rights and Access Control on customers in case of any cyber wrong doing is detected. This may be a gentle advise in the initial stages and get escalated to 2-3 repetitions. In case of continuation of wrongdoing, Big Friends must report the deviance to authorities.
    - For serious cases like terrorism/rioting immediate corrective directions will be very much in order and imperative.

- But the present version of Facebook Poke needs to be strengthened much more. However, when poking is done it should be given as a panel poke rather than an individual member poke to enable no enmity/ill feeling is kept against any particular person of Big Friends Panel. Panel Pokes can be :-
    - Advisory in nature on a pre-approved template/language
    - Cautionary in nature on a pre-approved template/language
    - Counselling in nature on a pre-approved template/language
    - Repudiatory in nature on a pre-approved template/language
- In case it is difficult to get the Big Panel as mentioned above, nominated geographical Data Brokers or Data Good Samaritans must do the job.
- Statistical poking can be a good tool to analyse Facebook as covered here.[24]

The advantages will be that Digital Compliances/Digital Governances will be strengthened without government directly getting a bad name. Today, the tendency is to find fault , starting and ending with government. The above outsourcing model will lead to better and effective online governance and generate lot of jobs.(Think it like a model of issuance of visas by VFS Global rather than US/UK/France Embassies directly in India)

Social Networking Sites(SNS)

The common security issues [25] observed in SNS are:-

a) Loss of user anonymity
b) Profile and personal information
c) Image Hacking and Image Tagging
d) Social Phishing
e) E Mail Spam Attack
f) Fake Profile dangers
g) Malware spreading like Koobface, Twitter worm, ProfileSpy worm etc.
h) Cross-Site Request Forgery and Cross Site Scripting
i) SQL Injections
j) Identity Theft
k) Cyber stalking and corporate espionage
l) De-Anonymization Attack
m) Identity theft

A. A. Obiniy et al bring out in their paper [26] that SNSs like Facebook, Twitter, MySpace and LinkedIn Social Networking Sites have provided users with platform for establishing and maintaining relationships from different points of life. The penetration of mobiles has even democratised the social media with diversified groups on several subjects including archaeology, sports, religion. Politics, current affairs, movies, education and many thousands of topics. The menace of cyber breaches can be tackled by using principles of data confidentiality, integrity and authentication. Cryptographic techniques go a long way in enabling the above methods.

Payments Digital Rights

Due to increased penetration of mobile apps and Internet across the world, the disruptions in traditional banking are a reality now. From the success of websites like policybazaar.com in India and PayTM ,the payments paradigm is also getting changed. In EU countries, adoption of PSD2 is driving increased business, competition and growth of Third Party Payment entitites.PSD2 has several provisions for ensuring better protection to customers for digital payments. Strong Customer Authentication(SCA) is really at the core to this regime. Principles of Knowledge, Ownership and Inherence enable fool proof system of payments. Some aspects of PSD2 [27] include:-

- Effective 13 January 2018
- Door opened to new entities called Payment Initiation Service Providers(PISPs) and Account information Service providers(AISPs)
- Leveraging of APIs enabled
- Almost real time fraud detection possible
- Only Euro 50 liability for customers in majority of cases, except wilful fraud/negligence cases

The Tyranny of Algorithms and Artificial Intelligence or a brave, new world of quick and unbiased decision making

Algorithms developed by IT companies are being used in various fields increasingly in various ways now by police authorities, healthcare, jurisprudence, HR headhunters. Though statistically speaking they may be " 80 % times correct" but that is of no solace to a person caught in Bengaluru Silk Board traffic jam by a police based on some developed algorithm. At that place all models will fail, not work. There has been mention of software COMPAS(Correctional Offender Management Profiling for Alternative Sanctions) developed in the US[28] which may have taken wrong arresting decisions/wrong punishing decisions/wrong digital decisions.

Real life is not of 0s and 1s, either or, black or white type. It is like a complicated logic and not straightforward. But, like Google Search with time algorithms may get better and better. The digital rights in these matters are still a grey area and possibly more work needs to be done to have a day when automated algorithms will rule our lives. The authors predict that non-human algorithms will be more helpful to bring full helmeted bike riders on Bengaluru's roads than police, reduce traffic rights violations at " non-zero tolerance" traffic junctions also, stop zig zagging of traffic, stop driving on "wrong side"(for some people increasingly driving on any side of convenience on Indian roads seems to be correct side) and other such issues. Hence

the brave, new world may bring us mixed bag. Indians will learn to adopt it the in the same way we are now patiently paying tolls on toll gates rather than with frowned faces.

Facial Recognition – Ramping up on the Aadhar success in India

Facial Recognition is getting a huge media space these days. Lot of credit for this must go to the success of sites like Facebook[29],LinkedIn,Instagram etc. They have popularised the democratisation of self-imaging in a big way. The template is now being planned to be replicated by security agencies, heath care/wellness industry, recruitment /hiring agencies, matrimonial services and others. There is a privacy cry on the issue but slowly and surely all of us will get imaged the way we all got Aadhar enabled.

Aadhar project of India has been a huge success story in India with more than a billion people having been issued Identity cards called Aadhar cards in India in last 2 decades. It is a verifiable 12-digit identification number issued by UIDAI to the resident of India for free of cost. Imagine Prime Minister of a country childishly weeping "I have been imaged. My face is about everywhere". Well, he/she cannot be since being a public figure. Slowly but surely common citizens will be going the same way. Their faces will have been captured by Government and private agencies from time to time. All citizens will have the "privilege" to be recognized by cameras/Internet/media/monitoring agencies/social media/polling stations and other places. The loss of privacy seems too far fetched. The citizens will have to be ready for "face recognition" in the same way as our VIPs are. The dilemma faced in Face Recognition encompasses points of view from many stakeholders. The needs, concerns and fears are amplified in a recent article[30].

Face Recognition has its pros and cons. These are tabulated below:-

PROS	CONS
Optimisation/Reduction in Security procedures at public places/gatherings	Images may be faked by malicious elements, but built in features can act as safeguard
Savings in time for compliant/good history individuals	Instantaneous rejection by potential recruiters/hirers/grooms on seeing faces with preconceived notions/bias/orientation
Good for morale as you check in to hotels/supermarkets/movie theatres and get welcomed,"HI,AMRISH,NICE TO SEE YOU"	Tyranny of faulty algorithms may profile a person wrongly in similar image scenarios(Ram and Shyam,Seeta and Geeta movies e.g.)
Credit rating style Facial recognition good score /points will be helpful for compliant individuals, but some may "buy the points"	Pressure of being compliant/regimented/correct all the time will make people enjoy less

As of April 2020,Face Recognition has acquired a sufficient traction and has the potential to be like Aadhar 2.0 in India and abroad. Consider the following recent successes/developments:-

- Over 1,900 faces[31] were recognized by Facial Recognition software by Indian Government during recent Delhi riots while President Donald Trump was on state visit in India. These people were involved in arson and destroying infrastructure. Only driving license and voter ID card were used for face identification of these culprits involved in Delhi Violence. This is being touted as huge success of Face Recognition in terrorism/rioting world. This template may definitely be a useful tool for governments of 21st century.
- San Diego Police in the USA is successfully testing[32] the Tactical Identification System, a mobile phone based Face Recognition paradigm where police can instantly recognise a person after taking image on smartphone and then compare and strive to get match pattern from an already available database of images.
- Updated Request Tender[33] from India's National Crime Records (NCRB),bids for which are expected by 27 May 2020, has elaborated/considered the various possible technical templates including for still images, scanned images and video image grabs of Face Recognition. NCRB has conceptualized the ambitious Automated Facial Recognition System (AFRS). Several good aspects from ISO Standard ISO/IEC 19794-5:2011 have been taken into consideration . This is an effort "in the direction of modernizing the police force, information gathering, criminal identification, verification and its dissemination" among various police organizations and units across the country. Also, the Facial Recognition System "is a great investigation enhancer for identification of: criminals, missing children/persons, unidentified dead bodies and unknown traced children/persons. It can provide Investigating Officers of the Civil Police with the required tools, technology, and information." The following aspects of Face Recognition have been included:-
  a. Varied lighting conditions.
  b. Small image sizes (300 x 300 pixels)
  c. Low Jpeg image quality.
  d. Plastic Surgery
  e. Aged Images
  f. Bearded faced images
  g. Makeup images
  h. Slanted Face
- Adoption of Digi Yatra[34] Face ID methodology increasingly at major Indian airports is bringing ease, convenience and faster transits at India's airports now. Bengaluru,Hyderabad are using the system smoothly wherein Face recognition helps in doing away with lot of paperwork and optimised times for passengers and airports.

- Attendance Management[35] in educational institutions is bringing more automation, better visibility and optimisation and removing the chaos of human bias if any of teachers.
- An innovative way of doing sentiment analysis/mood analysis/morale management in business is being done in South Africa by a Johannesburg based startup Camatica[36].The face recognition software is able to "read /analyse/capture" the sentiment and mood of the employees from face reading to enable management to do corrective actions/course corrections.
- UAE Security operations have received a big boost towards Face Recognition[37] recently. The authorities there have ordered 50 Vuzix Blade Smart Glasses, powered by NNTC's trademark technology. The security forces wear these glasses and then scan faces in a crowd and compare/match/discern them against an approved database of violators/ missing people/ suspects/other miscellaneous studies. The vendor claims an almost 98 % true match pattern based on prestigious NIST certification.

Fig. 10 Face Recognition is being leveraged in many ways across many countries

Face Recognition: Implementation/Methodology

The algorithms/methodology of Face Recognition use the following[38] sequential steps:-

a) Input the image.
b) Face Detection
c) Face Extraction
d) Face Recognition

Approaches towards Face detection techniques include techniques[39] using Eigen face, Artificial Neural Networks (ANN), Support Vector Machines (SVM), Principal Component Analysis (PCA), Independent Component Analysis (ICA), Gabor Wavelets, Elastic Bunch Graph Matching, 3D morphable Model and Hidden Markov Models. More and more work is emerging on this trending topic on regular basis.The details will be discussed in a future paper.

Conclusion

Internet in last 2 decades was in evolutionary phase. It was like Wild West version of cyberworld. The regulations were few, freedom unlimited and scope for innovation/disruption more. But as happens to any Greenfield area in our cities/towns, the regulation will be more and more. But the privacy issues have acquired an unstoppable momentum now. A healthy balance of regulation and privacy will be necessary for all stakeholders in the new world. With the coming trend of Face Recognition gaining ground, the world will be required to get used to be more open and transparent regime akin to VIPs/celebrities.

Acknowledgement

The author acknowledges the efforts of all the IT/cybersecurity/healthcare professionals and authorities from several Bengaluru based organisations for their valuable inputs.

About the Author

The author is an accomplished Industry and Academic professional having vast experience in Operations,Quality Assurance,Academics and has served across the vast country India over three decades. The author has several papers to his credit. He is an alumnus of prestigious IIT,Madras.

Bibliography/Webography

1. A look at data breaches, cyber-attacks India saw in 2019, Deccan Herald, 16 Dec 2019
2. Lawless-The Secret Rules that govern our digital lives,Nicolas P.Suzor,Cambridge University Press, June 2019
3. Privacy's Blueprint:the Battle to control the design of new technologies,Woodrow Hertzog, Harvard University Press, 9April , 2018
4. The Age of Surveillance Capitalism :The fight for Human future at the new frontier of Power,Shoshana Zuboff,New York,2019
5. General Data Privacy Regulation(GDPR) , https://gdpr-info.eu/
6. Pseudonymisation , https://www.thalesesecurity.com/
7. How to de-personalise data,https://tdwi.org/articles/2018/06/06/biz-all-gdpr-and-tokenizing-data-3.aspx

8. Overview of fines and penalties, https://www.enforcementtracker.com
9. The Directive on security of network and information systems(NIS Directive), https://ec.europa.eu
10. California Consumer Privacy Act, Fact Sheet ,https://oag.ca.gov/system
11. Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines, https://www.iso.org/obp/ui
12. Social media privacy Protection and Consumer Rights Act of 2019, https://www.congress.gov/bill
13. The Personal Data Protection Bill introduced and referred to Standing Committee,11 Dec 2019, https://prsindia.org/billtrack
14. Law to curb deliberate online falsehoods takes effect, 02 October 2019,https://www.channelnewsasia.com/
15. Wuhan virus: Govt debunks fake news on Singaporeans contracting the virus and Singapore running out of masks,The Straits Times,31 January 2020
16. Online content:To regulate or not to regulate – is that the question? https://www.apc.org/en/pub
17. Needless Network Disruptions: A Continuing Menace to Online Rights in Africa,*June 20, 2019*,https://www.africafex.org
18. Six Months of Obscurity: Chadians Digitally Cut-Off, September 4,2018 https://www.africafex.org
19. Disenchanted Liberians Recount First Social Media Blackout Experience *June 13, 2019*, https://www.africafex.org
20. A step closer to realising internet freedoms in India: Supreme Court rules indefinite internet shutdowns are unconstitutional, January 2020,www.apc.org
21. Social media faces EU fine if terror lingers for an hour,www.bbc.com, 20 August 2018
22. Australia suddenly passes new laws regulating streaming of abhorrent violent material by ISPs and other content providers,www.dentons.com,15 April 2019
23. Government introduces data protection bill in Lok Sabha, to send it to joint select committee, The Economic Times,11 December 2019
24. Poking Facebook: Characterization of OSN Applications Minas Gjoka, Michael Sirivianos, Athina Markopoulou, Xiaowei Yang University of California
25. A Survey of Various Security Issues in Online Social Networks, M. Milton Joe and Dr. B. Ramakrishnan, International Journal of Computer Networks and Applications Volume 1, Issue 1, November - December 2014
26. Social Network and Security Issues: Mitigating Threat through Reliable Security Model, A. A. Obiniyi, International Journal of Computer Applications (0975 – 8887) Volume 103 – No.9, October
27. The revised Payment Services Directive(PSD2) and the transition to stronger payments security, https://www.ecb.europa.eu/
28. A Popular Algorithm Is No Better at Predicting Crimes Than Random People,Ed Young,The Atlantic,17 January 2018
29. Why Facebook is beating the FBI at facial recognition, 07 July 2014,https://www.theverge.com/
30. Whose side is face-recognition technology on? Roshni Majumdar, India Today, 7 November 2019
31. Delhi violence: Over 1900 faces recognised through facial recognition, says Amit Shah, The Economic Times,13 March 2020
32. Facial recognition, once a battlefield tool, lands in San Diego County, Ali Winston,www.revealnews.org,7 November 2013
33. Request For Proposal to procure National Automated Facial Recognition System (AFRS), National Crime Records Bureau (NCRB) Ministry of Home Affairs Government of India,28 June 2019
34. KIA launches 'Kerb-to-Gate' biometric pass,Facility available first to Vistara passengers, who can breeze through till boarding. Rasheed Kappan, Deccan Herald, 23 July 2019
35. Attendance Management Using Facial Recognition ,Rajath S Bharadwaj, Tejus S Rao, Vinay T R, International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8 Issue-6, April 2019
36. SA startup launches facial recognition software that analyses moods, Dhivana Rajgopaul, www.iol.za,29 July 2019
37. UAE's law enforcement utilises AI-powered face recognition system,Jess Phillips,www.intelligentcio.com,27 June 2019
38. A Study of Factors affecting Face Recognition ,Aayushi Bansal, International Journal of Advanced in Management, Technology and Engineering Sciences,Volume 8, Issue II, Feb 2018
39. Study of Face Recognition Techniques: A Survey, Madan Lal et al., International Journal of Advanced Computer Science and Applications, Vol. 9, No. 6, 2018