LEGAL ISSUES LOOMING LARGE ON AIRPORT SECURITY CHECK

Bikashita Choudhury[1]

ABSTRACT

This article focuses on the technologies used during airport checking and its pros and cons. It also throws into light the different practises of various countries for security check and how these rights hinder basic human rights. The article brings forth the drawbacks of the technologies that are currently being implemented in aviation sector and also includes some of the personal accounts of individuals who felt vulnerable at the hands of these measures. India being one of the most prospective countries, on the verge of implementing such procedures should consider these problems as a forewarning and a cue to develop as well. The article concludes with some discussion of latest technologies that can be introduced to keep some damages in check.

keywords: biometrics, iris scan, finger printing, database, video surveillance, explosive detection system, RFID, privacy, body scanner

[1] KIIT School Of Law, Bhubaneswar (India)

INTRODUCTION

"Any sufficient advanced technology is indistinguishable from magic"

These words by Arthur C. Clarke still hold true in our society, having had their fair share of dire consequences. No doubt technology has taken us to places, has reduced human toil and labour, done away with many impossibilities, yet the ill effects of technology are much more than asked for. To deal with technology and its entanglement with legal issues we would probably put forth a never ending list of do's and don'ts and create a more confusion regarding its use and abuse.

Law has been trying to bridge the gap between use and abuse of technology by ensuring that development does not slow down on one hand and on the other hand the ill effects of technology are reduced to the minimum. The approach adopted by law to let a technology progress and then impose restrictions on it has affected different bodies trying to implement technology in their respective sectors. One of such sectors, to face the heat of over use of technology is the airport sector. The new implementation of technology following the 9/11 attacks on U.S.A and their plan to sabotage the airport itself has led to a rising concern among the government bodies all over the world. The transportation security administration body of U.S.A has implemented many rules and also introduced latest technologies at a large scale in an attempt to beat down the plots to disrupt the smooth processes of the flights.

THE TECHNOLOGIES INTRODUCED AND THEIR UTILITIES

Biometrics:

Biometrics is that branch of technology that is most effective in the identification of an individual by help of biological characteristics and traits. Physiological characteristics are mainly categorised by the biometrics department set up in the airports.

Biometrics is perhaps one of the most fast emerging technologies that has been put to use not only by the govt. of India (to a bare minimal) but also all over the world. Ranging from the *aadhar card* to tracking employees at five star hotels as well as for maintaining the security of their guests, the countries have done it all to ensure that they are protected from any privacy threat; but then the real question arises when these voluminous records obtained from biometrics such as-iris scan, finger printing, facial images are kept as backups in many working places. While keeping a check and to ensure a hassle free journey there has to be a huge back up of all these data, there still remains a nagging suspicion at the back of our minds -"Is it all really fail safe? Can the government truly assure that our data are protected from all sides? If so, then why is the govt. always facing the blaze trying to protect our documents and it goes to a frenzy when suddenly one fine morning they find out that there is a huge anomaly in a bank account? If the computer system and data storage system is so weak then obviously it is a herculean task to store all the data and it must be under some pertinent threat." To talk about it the question comes up again: what prompted the Government of India to list the Civil aviation sector, railway passenger reservation system and communication network, port management, companies and organizations in power, oil and natural gas sectors, banking and finance telecom sectors as critical apart from certain strategic government departments such as space(ISRO), External Affairs Ministry(*passport database*), the Home Ministry's police and intelligence networks, the Prime Minister's office(PMO), the NSCS and the cabinet secretariat.[2]

The use of biometrics in airports does not only end with finger printing but it also extends to video surveillance, facial recognitions, palm printing and iris scan and retina scan as well.

Explosives detection system[3] is another technology that is put to use in the airport security check for baggage (to check unopened luggage). This system is used to only check the risk of explosives being carried on board. These are computed tomography x-ray machines which interpret data from multiple x-ray diodes. They make use of software data to get information from these diodes. This is one system introduced by the airport officials that has reduced the task of repetitive checking and also has brought down human labour to a great extent. With the advancement in technology it has improved in terms of speed, accurate analysis and easy check-ins as well.

THE ILL-EFFECTS OF TECHNOLOGY

There are certain threats posed by Biometrics, which are:

i. The system of biometrics, though hugely based on facial recognition, hand printing and collecting of details, have a lasting impact on the individual data that are kept as a backup. The job of the airport security and searching once handed over to private companies, proved to be disastrous. They started keeping huge backup for ease as well as comfort of passengers. Though it was well received by the travellers at first but then after some time it also gave rise to several issues, one of them being the fact that it made the data of all individuals available-just a click away waiting to be used and

[2] S joshi, "*Waking up now, India up to cyber security strength*"; The Hindu, 14 (Bangalore, 19/07/ 2013)

[3] Ex-post Evaluation of PASR Activities in the field of Security Interim Evaluation of FP7 Research Activities in the field of Space and Security Aviation Security and Detection Systems - Case Study January 2011, pg 5

abused to the whims and fancies of anybody and gave rise to the probability of the situation of swapping ones identity to such an extent that it might never be regained.

ii. The introduction of a full body scanner post the 2009 panic that raised a concern worldwide when a bomber with a liquid bomb with himself was able to board a U.S. bound flight and the passengers fought tooth and nail to defy his attempts while the plane flew over Detroit, Michigan[4] was perhaps one of the decisions which seemed most suited to the current situation but it met with many raised eyebrows later on as the speculation of full body scanners being able to peer inside clothes and check out any medical surgery such as breast enhancements or similar scars gradually proved to be true. That is not the end of it, security checks are followed by a plethora of questions which is more embarrassing. Even those willing to go under the scanner started to recoil thinking about the prospect of dealing those personal queries.

iii. To talk about this aspect who can forget the incident of bollywood heart throb **Shah Rukh Khan's embarrassing account of travel to U.S.A.**[5] followed by a confession of some staffs of the airport security department that almost semi naked images of the superstar was not only printed but circulated as well among the staff members of the security check arena and more over the search was carried out by a woman instead of a male operator by defying the rules set up by the department itself.

iv. No doubt that biometrics is the brain-child of many eminent scientists of the world, yet it is recent and fallible, not exactly full proof. Even if there is a glitch in one of the smallest set ups it might lead to an entire machinery failure in a security department. Then what? The airport security check cannot wrap up itself entirely and go on a vacation giving a petty excuse of a defunct machinery!

v. At the same time the accuracy rate of biometrics matching rate is not trust worthy. There are two types of problems arising from such machines-

i) false match ii) false non-match

Biometrics were basically designed to perfectly match one's data. Every time it is put forth, these kind of algorithms despite being theoretically possible have not been achieved practically just because of one simple reason:

There is always some difference in each specimen signature of an individual despite one's best attempts.

[4] Terror Attempt Seen as Man Tries to Ignite Device on Jet Available at: www.nytimes.com/2009/12/26/us/26plane.html last seen on 29/04/2014

[5] Shah Rukh Khan Claims Naked Body Scanner Images Of Him Were Printed, Circulated By Airport Staff Available at: http://www.huffingtonpost.com/2010/02/10/shah-rukh-khan-claims-nak_n_457200.html last seen on 30/01/2014

False match occurs when two biometric data of entirely different persons are given as the same. False non-match occurs when the same biometric data of one single person is given to be different. This occurs because the system calculation is based on statistical records. The percentage of accuracy varies. This also poses another crucial question- how can such a defunct system be installed in high security sectors?

vi. In recent times there has been problems regarding smooth use of biometrics. As it is intently attached to the physical attributes of an individual, there are some cases of anomalies where the finger prints of some individuals just don't come up well. It creates a trouble for others raising some suspicion about the minority class.

vii. The collection of biometric information also raises some health and safety concerns. There are number of medical conditions that can affect iris biometrics. A study was conducted by engineering moguls on how image of the iris is affected by cataract removal.[6] It involved a number of patients who had their eyes photographed thrice before surgery and afterwards. After surgery, six of 55 patients were no longer recognised by the computer from their iris pattern. The study concluded that after cataract removal surgery people should re-enrol in iris biometric systems. Similar effects to that study may be caused by laser iridotomy.[7] Laser iridotomy is used to correct the angle-closure caused by glaucoma and uses a very focused beam of light to create a hole on the outer edge of the iris, thus destroying the original iris pattern. Additionally, some blind people will have trouble aligning their iris with the scanners and wheelchair users may have difficulties due to the location of cameras and insufficient height variation possibilities although handheld or height-adjustable cameras can cope with this problem[8].

RIGHT TO PRIVACY AND BIOMETRICS

The American civil liberties union has blatantly termed it as a "virtual strip search" and "an assault on the dignity of passengers". The technology put in use is back scatter wave rays or the millimetre wave technology. These wave rays are made to incident on an object, they reflect back to varying extent by the muscles and bones. These images reveal not only weapons, explosives and

[6] Roizenblatt R., *et. al.*, "*Iris recognition as a biometric method after cataract surgery*,"2, BioMedical Engineering OnLine, (2004 Vol.III, issue 1).

[7] European Commission, *Biometrics at the frontiers: Assessing the impact on society*, Institute for Prospective Technological Studies, February 2005, Technical Report EUR 21585 EN

[8] European Commission, *Biometrics at the frontiers: Assessing the impact on society*, Institute for Prospective Technological Studies, February 2005, Technical Report EUR 21585 EN

concealed drugs, but also ‘rolls of fat, the size of breasts and genitals, and catheter tubes’.[9] That creates vulgar images of an individual throwing into prominence the varying features and detailed contours of a human's body. Many a times there has been complaints of passengers about the airport officials gawking at those obscene images and snide comments as well. Many passengers are also subjected to full body pat down even after body scan because of presence of trivial things for example a hair band in one's pocket which the body scanner can pick up.

These kind of screening pose a question mark on the screening and check of those passengers who are differently able: for example using prosthetics. It is the right that the dignity of each individual be maintained even while travelling. To endure a full body pat down is equally painful as is the screener because it will pick up any prosthetics used. Those group will always be under the scanner and raise suspicion in the minds of TSA agents.

As promised by the government that the checking is to be carried out by people belonging to the same sex category as of the individual being checked, it poses a problem for the transgender as well.

Even more serious is the laws on child protection. On January 10, 2010, the Guardian newspaper came out with a statement that, “new scanners break child porn laws.” According to them the creation of these images are “virtual strip searching”. Children in UK need not go through scanners like everyone as the legal situation clarifies. Yet there lies a number of problems . To avoid a breach in child pornography, those under 18 must be exempted from going through scanners. Can terrorists not be younger than 18? The only alternative is : bring in a legislation ensuring that airport security staff are exempted from prosecution.[10]

The Checks and measures as claimed:

Despite promises by the authority and other people that there won't be any oddity involved yet people can take images of these scans and save them in their cameras and phones. Despite repeated claims by the airport authorities that the scanner that they are supplied with are without any facility to store, transfer or print data yet the social service groups are not assured. The images are supposed to be automatically deleted after every scan and the face is supposed to remain blurred. The scan is to be carried out by a person of the same sex and the agent checking the images are located in separate cubicles away from the checking zone.

[9] S. Kornblatt, ‘Are Emerging Technologies in **airport** Passenger Screening Reasonable under the Fourth Amendment?’ (2007) 41 *Loyola of Los Angeles Law Review* at 390

[10]Charlotte Harwell, Ethical issues surrounding the use of biometric body scanners in airports (Cesagen, Lancaster University)

Now to talk about passports, it makes use of RIFD technology, it is perhaps one of the most beneficent boons that came along with the introduction of technology into airport practise. This was first introduced for the benefit of travellers for ease of custom clearance and also "real time tracking of their luggage". There are chances of commercial danger and privacy infringement as well. Once any document bearing a RIFD technology chip is put through a scanner, it takes down all the detailed documents of an individual and at times more than that is necessary. Here comes in the permanence or quasi permanence of these kind of data backups.[11]

THE CONLFLICT WITH LAW:

The main types of violation of rights that arises are:

i) violation of right of privacy

ii)injury to the person or to legal interests[12]

iii)injury to religion

THE ENLISTED LAWS AND THEIR VIOLATION

The infringement of rights due to this procedures in various nations:

Right to privacy in India

Section 43 of the information technology act also to some extent prevents and penalises anybody if there has been an unlawful access to some one's computer or database :

43. Penalty for damage to computer, computer system, etc.- If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network,-

(b) downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;

[11] Alan s. Reid, journal of trade and international law policy(2005)

[12] Airline passenger security screenings: new technology and implementation issues, (1996) The national academic press, at 34

Right to privacy in India as guaranteed by our constitution:

As given in the Indian constitution, under article 21: right to privacy is one of those momentous rights conferred to us.[13]

If we come to the International concepts of privacy:

According to *Black's law dictionary* privacy means right to be let alone, the right of a person to be free from unwarranted publicity, and the right to live without unwarranted interference by the public in matters in which the public is not necessarily concerned.

A more dramatic change comes along in the form of Section 43A which is a recent amendment made in the year 2009. It provides a Compensation for Failure to Protect Data. In India this protection brings under its ambit not only a citizen but also a foreign individual. They can sue a BPO or ITES Service provider for negligent handling of data.[14]

Article 12: Universal Declaration of Human Rights (1948) :

"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."

Article 17: International Covenant on Civil and Political Rights (to which India is a party):

"No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home and correspondence, nor to unlawful attacks on his honour and reputation."

Art.8: European Convention on Human Rights:

Everyone has the right to respect for his private and family life, his home and his correspondence;

There shall be no interference by a public authority except such as is in accordance with law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the protection of health or morals or for the protection of the rights and freedoms of others."[15]

The Take Of The European Union:

[13] "no person shall be deprived of his life or personal liberty except according to procedure established by law.

[14] Cyber law: Indian and international perspective, Aparna Vishwanathan, ch 8,provisions of Information technology act,2000

[15] N.S. Nappinai, adv., Privacy and the Constitution, nappinai and co.,founder member:technology law forum

The European union likewise has taken the necessary steps to combat with the chaos that has arisen due to the use of biometrics as well, but the question remains to what extent has they been useful:

Newer tools:

The communication "New tools for an integrated European Border Management Strategy" puts forth suggestions for modern technologies that would constitute an integrated part of the European Border Management for future, including:

- introduction of an entry and exit system, electronic record of dates of entry/exit of third-country nationals
- facilitate crossing of border for bona fide travellers by introducing automated border crossing facilities for EU citizens and some third-country nationals
- setups and equipment for an Electronic Travel Authorisation System.

Check third country arrivals:

The Commission would like to see an entry and an exit system that applies to the nationals of third-country admitted for short stays (for three months). The system includes the recording of information on time, place of entry, length of stay as authorised, as well as the transmission of automated alerts to competent authorities, if a person is identified as "overstayer" anytime this occurs.

The nationals of the third country those who require visas have to provide their biometric data for the VIS when applying for a visa at a Member State's consular post; border crossing points are equipped with necessary equipment to allow verification of the identity of the visa holder based on those data. In order to minimise the impacts on border checks as well as take full advantage of the investments, it is reasonable to await the successful and full rollout of the VIS(visa information system).

Protection:

Systems introduced must be in conformity with EU data protection rules. Specific care must be taken to ensure compliance with the Arts 16 and 17 of Directive 95/46 on confidentiality, security as well as network security and confidentiality laid down by Regulation 45/2001.

The data should be used by competent immigration authorities. Individuals should have the right of access to information held on them, and to challenge and correct this information as provided for in Community and national legislation. Provisions for an appeal mechanism in cases where third-country nationals are "forced" to overstay should also be introduced.

The Registered Traveller Programme must be made subject to the same requirements on data protection. Data protection provision, right to personal information used to justify refusals of applications would be appropriate. The Programme should also include a requirement that authorities provide reasons for refusal and an opportunity for applicants to appeal against refusal.[16]

Other countries as Canada:

The Canadian Charter of Rights and Freedoms:

`Everyone has the right to be secure against unreasonable search and seizure.'

New Zealand:

Sec. 21: *New Zealand Bill of Rights*: `everyone has the right to be secure against the unreasonable search or seizure, whether of the person, property or correspondence or otherwise.[17]

The Glitch:

The US. constitution has no express rights to privacy though the amendments reflect some aspects of privacy such as privacy of belief, privacy of home ,privacy of person and possession against unreasonable searches...but since the search carried out is due to the ensuring of security of thousands of passengers travelling in hordes the amount of intrusion and breach is almost negligible as according to the judges of many US. high courts and also to many Americans.

Though the securities and checks are meant for the protection of the people of America only, they themselves are no exception to all those harassment piled upon the travellers. To take refuge one can very well claim that the supreme court has held that there is a fundamental right to travel and to interstate migration within US. Therefore, the laws that prohibit or burden travel within the U.S. must meet with strict scrutiny. In the *slaughter house case* in 1837, justice Doughlas had stated "the right of person to move freely from state to state ...is so fundamental...The right to move freely from state to state is an incident of national citizenship protected by the privileges and immunities clause of the fourteenth amendment against state interference.[18]

In India even the protection forwarded to data security is largely flawed. Section 43A only refers to body corporate and excludes natural person from its purview. According to the Department of Science

[16] EU Focus Commission presents vision for integrated European border management system 2008
[17] N.S. Nappinai, adv., Privacy and the Constitution, nappinai and co.,founder member:technology law forum
[18] Erwin Chemerinsky, constitutional law principles and policies (aspen publishers 3rd ed.) at.857&858

and technology, it is trying to satisfy clients outsourcing to India or using call centres. Accordingly, the term body corporate as defined clearly excludes individuals.[19]

So any kind of breach of privacy carried out by an individual with the help of technology is difficult to prove and indemnify.

Religious objections:

In the U.S. itself there has been many religion based objections regarding the use of biometrics. " The objection is based on language in "Revelation":

> [The Beast] causeth all, both small and great, rich and poor, free and
>
> bond, to receive a mark in their right hand, or in their foreheads:
>
> And that no man might buy or sell, ... and his number is
>
> six hundred, threescore, and six. (Revelation, 13:16–18.)

Some Christians are of the opinion that the biometric is the brand discussed in Revelation and biometric readers as the only means of viewing these brands. . In Alabama a few people objected to providing an SSN for driver's license as required under Alabama law. The individuals claimed that their refusal was based on religious beliefs that prevent them from having an SSN. This case is pending in the Alabama state courts (Alabama Lawsuit, 2000).

Another threat that people have embraced unwittingly is the *registered traveller program*, it is a concept that was introduced for the ease of passengers-it is mainly a self submission of information through biometrics which creates a backup of a specific individual in the database of the airport's computer thereby enabling him to just breeze through the security check in future course of travels. They have been part of the U. S. based programmes like GLOBAL ENTRY and CLEAR which carried out an extensive underground check on frequent fliers who gave their approval.

The UK Borders Act 2007 and eye-prints

The UK Borders Act 2007 enables a compulsory identity card for non-EU nationals and this will require immigrants to submit a biometric document that includes 'features of the iris', effectively giving rise to an 'eye print' database. Iris recognition has been on trial in UK airport since 2005 but this trial

[19] Cyber law: Indian and international perspective, Aparna Vishwanathan, ch 8,provisions of Information technology act,2000

reported that iris-scanning technology is not up to the standard required to sustain the ID card scheme[20].

THE HAZARD THAT TECHNOLOGY POSES

Biometrics present a greater potential for function but is a threat as well because biometrics offer an ability to track anything in a way that current passwords and PINs cannot.[21]

Here comes the main issue of maintaining the data secrecy. Today everything is available over the internet, when you store the data of an individual, it is your responsibility to maintain its secrecy as well. Initially, this was a both public and private initiative by the U. S. government but now it has become an entirely private venture though the security department continues to remain under the TSA.

Because fingerprints is the unique way of differentiating data. It's used as primary key in their database. A fingerprint corresponding to a valid passport will give details of the passport and issued visas. Now that visa detail is used to check his flight details etc.

So for every country they have their own database all information regarding travel logs, visa details, passport holder information etc in a single database handled by a mainframe server. Now that is connected to a frontend server to which airport authorities are connected and logged in to work all these verification thing. Backup of the main database is highly necessary.

One type of backup would be storing in the backup database as soon as modification to the main data base is made.

Backup done each day for, say, 6 days, and on the 7th day i.e. entire weeks changes are backed up. They can back up it as entire data base every time a maintenance work is performed. They can also append the new entries to the backup and update the modifications only. A log is kept of all backup tasks, mainly for the changes recorded in the backup.

Since there remains a lot of computers connected to one another in order to continue such a huge set up, it increases the possibility of MITM attack. These kind of attacks are quite common as the mode of 3 way handshake is automated in connecting of P.C.s. More over if a socket is insecure , it is easy to plug in fake I.P. address and port and you are in.

SQL injection is very easy to be used (removing ones identity or swapping). Exploiting security vulnerability in a database driven website / server. Inputs are made such that commands are executed on the database as the attacker wants.

[20] Sally Ramarage, Criminal Lawyer, **The emperor's new clothes,** 2009

[21] John D Woodward jr. et. al., Army Biometric Applications,(RAND publication 2001) at 28

An attacker will have to break in the airport officials LAN and get access to a PC. Then they would launch a secure shell and do whatever they want.

To get information from the database, attacker only needs to bypass 1 or 2 firewall. From there he can fake his connection as authentic one and take control of the database.

The chips on the passport can be hacked by Radio frequency intrusion talking away its digital signature or key information. So it can be used to guess passwords or impersonate anyone.

Radio frequency is so produced such that small chips like those of passport or SIM card's data can be accessed. It's possible without physically connecting. Radio waves that do all the work-connecting, breaking in, data extraction, data transfer and closing connection. one can think of it as *one Sided Bluetooth connection* where I do whatever I want with your phone after connecting to it forcefully. That's much like connecting to a **Wi-Fi** network by breaking its password, or accessing social sites in college network by bypassing its firewall. To explain a situation, it can be said that all that an attacker needs to do is eavesdrop on the reader's radio communication while getting a clearance at the security check section. These kind of use of biometrics always leaves a trace as well and now a days due to every details being enlisted on the net, it is easy to track any individual via those information collected from any database centre at any airport. The data collected can be then used to create a new passport and gain a social security number and one can never get the trail of his finances!

THE TAKE OF COURTS ON SUCH ISSUES

Michigan law review also quoted on this problem: (vol. 72:118)

The number of cases contesting the constitutionality of airport have greatly increased during the past year but courts have often failed to give questions presented the careful analysis that they deserve. To date most decisions citing the overwhelming social interest created by the imminent danger of passenger death held that searches do not violate the fourth amendment. A few courts have however maintained that established search and seizure law simply cannot be stretched far enough to approve these searches in their present form. None of these are perfectly analogous to present airport procedures. Therefore if airport searches are to be allowed ,either the procedures must be modified to fit the established exceptions or a new exception to the warrant requirement of the fourth amendment must be created.

A lawsuit brought by a Washington-based privacy group had argued that full body scanning technology violates, among other federal laws, Fourth Amendment protections from unreasonable searches because the scans are more invasive than necessary.

The court disagreed with the group in a 3-0 rejection of their suit, contending that intrusions on individual privacy must be balanced against promotion of legitimate government interests. “The need to search airline passengers to ensure public safety can be particularly acute,” the court wrote in its ruling. Body scanners, unlike other forms of screening technology, are “capable of detecting, and therefore of deterring, attempts to carry aboard airplanes explosives in liquid or powder form,” the court stated. The court also determined that the Transportation Security Administration improperly deployed the technology in 2007 by failing to give notice of its plans to the public.[22]

Despite the TSA and US government extensively supporting these set ups, it finally has started to feel the heat as well.

EPIC[23] has obtained an order from court instructing the Department of Homeland Security to undertake a public notice on rulemaking. On July 2, 2010, EPIC petitioned the D.C. Circuit Court appealing to suspend the body scanner program, stressing its main assertion " TSA has acted outside of its regulatory authority and with profound disregard for the statutory and constitutional rights of air travellers." EPIC proclaimed that the controversial programs violated the Administrative Procedures Act, Privacy Act, Religious Freedom Restoration Act, Video Voyeurism Prevention Act and the Fourth Amendment. On July 15, 2011, the D.C. Circuit Court of Appeals ruled that the agency had actually violated the Administrative Procedures Act by implementing body scanners as a primary screening method without first undertaking public notice and comment rulemaking. The Court ordered the agency to "promptly" undertake proper rulemaking procedures and also allow the public to comment on the body scanner program. To date, there has been no such visible progress on behalf of the agency in this regard.[24]

Despite the EU Regulation and US Consumer Privacy Bill Of Rights clearly chalking out stringent measures such as "data minimisation principle", "right to be forgotten and right to erasure", "use limitation" and "collection limitation"[25], the question remains: what is the standard measure to determine such guidelines. How much collection and use of data will provide security? How long the retention of data can be termed safe? The answer inevitably is "none".

[22] Court Rules On Airport Body Scans
Available at: http://blogs.wsj.com/law/2011/07/15/court-rules-on-airport-body-scans/ accessed on 15 August 2013

[23] it is a private health care software company

[24] Court Rules On Airport Body Scans
Available at: http://epic.org/privacy/body_scanners/epic_v_dhs_suspension_of_body.html accessed on15th August 2013

[25] Report of the Group of Experts on Privacy (Chaired by Justice A P Shah, Former Chief Justice, Delhi High Court)Government of India, Planning Commission

There has been recent developments where TSA itself has started to remove body scanner devices with regard to the claims of many that they emit a small amount of ionizing radiation , which if exposed to for a longer period, can lead to cancer. Also at the same time, body images that need to be reviewed each times slows down security check up.

The European union also took back this initiative in order not to risk the health and security of its citizens.[26]

One author who explored "whether the use of such X-ray devices in the United States breaches the Fourth Amendment" has concluded that much will depend on whether the making of images is judged to be 'unreasonable'. Given the perceived dangers from terrorism in air travel, their use may well be held to be reasonable.[27]

THE INDIAN SCENARIO

It can be seen that GOI intelligence or info-tech agencies of India have not indigenously created, tested and certified a firewall for system and database security. The firewalls that are in use are purchased commercially from international info-tech vendors. So it is just a cake walk for an employee who has designed the GOI's firewalls to provide key information of the same for personal gain.[28]

To talk of Indian perspective, it is about to introduce RFID technology as early as 2015. With India being lackadaisical in introduction of stricter security even at railways after repeated attacks, is miles behind in lapping up security measures at airports. To introduce this kind of technology in India without having proper resources to check its ill use can have a drastic effect on India's security system.

As of now India is set to introduce body scanners that would work on millimetre-wave technology. The scanners, which are a recent invention, do not emit any kind of harmful rays and a stylised image is created after the rays bounce off the top layer of skin. Any abnormality in the body contour, which could mean hidden explosives or weapons, will be visible on the screen for both the passengers and the security official manning it.

This scanner does not produce an image where body contour and shape is visible and only a generic image is generated. As India has taken cue from the developed nations and introduced the better

[26] TSA Removes X-Ray Body Scanners From Major Airports Available at: http://www.propublica.org/article/tsa-removes-x-ray-body-scanners-from-major-airports accessed on 15th August 2013

[27] Pamela R. Ferguson and Fiona E. Raitt, "If a picture paints a thousand words...": the development of human identification techniques in forensic anthropology and their implications for human rights in the criminal process 2013 International Journal of Evidence & Proof

[28] S G vombatkere, 'cyber security, surveillance and democracy', Mainstream, (june 28-july 4th) (2013) at 5

version of the technology, it should also implement laws before hand and prevent the chaotic situation that has arisen in the western countries. [29]

India not only faced trouble with its citizens but important personalities have many a times been subjected to many harassments:

India's ambassador to US has once been pulled from an airport security line and frisked by a security agent in Mississippi. The hands-on search took place even after Meera Shankar's diplomatic status was revealed. According to some reports Ms Shankar, who was on her way from a conference, was singled out because of the fact she was wearing a sari.[30]

Mr. A P J Abul Kalam had boarded an Air India flight at New York's JFK Airport. He was already subjected to “private screening,” as his name is not enlisted under the category of dignitaries exempt from security screening under the American guidelines.

However, after he entered the aircraft, U.S. security officials came and asked for his jacket and shoes, claiming they were not checked accordingly. With Mr. Kalam's consent, Air India staff then gave the same to American officials. It is not known whether these items were rechecked by any Indian security personnel before being returned.[31]

These technologies no doubt has played a major role in bringing down threat of attacks all over but with time people have learnt how to defy these machines as well. There has been repeated news of travellers getting past the security check with objects in possession that are not allowed, complaints of these security checks being biased towards the Muslim countries and bordering on the line of abuse to many people who bear distinct surnames.

Indians living outside has also been victims of these kind of hassles:

In an unique case in Poland, a Sikh was asked to remove of his turban and allow it to be taken through the x-ray scanner was not taken lightly. As narrated by him:

[29] Airports to install scanners that don't show body contour
Available at: http://www.indianexpress.com/news/airports-to-install-scanners-that-dont-show-body-contour/1151248/ accessed on 26th August 2013

[30] India's ambassador Meera Shankar frisked at US airport
Available at: http://www.bbc.co.uk/news/world-south-asia-11957943 accessed on 26th August 2013

[31] U.S. ‘regrets inconvenience' after Kalam faces double security check
Available at: http://www.thehindu.com/news/national/us-regrets-inconvenience-after-kalam-faces-double-security-check/article2624194.ece accessed on 26th August 2013

"The Judge viewed the CCTV footage of the five or so incidents in which I had been stopped by the Warsaw Airport Border Guards. The CCTV showed clearly that I followed all the usual steps in preparing to go through the Security check – i.e. hand over my lap top, briefcase, watch, Kara, belt, metallic objects, belts etc and placed them on the scanner. The Guards are seen asking me to accompany them to a separate cabin which does not have CCTV – in that place (rather a claustrophobic area) the Guards start to harass me demanding that I remove my turban… my protestations that they should first check me with the hand held detector are not recorded, but the Guards ignore my requests .. and I am forced to remove my turban – else I would not be able to travel".[32]

CASE STUDY:

The famous case of Jeffery H. Redfern and Anant N. Pradhan v janet napolitano, in her official as Secretary of Homeland Security and john pistole, in his official capacity as Administrator of the Transportation Security Administration, was one of the curtain raisers where the court had to allow the case in America thereby quashing many instances of cases not allowed to be registered due to lack of jurisdiction of courts. The plaintiffs argued though most of objections forwarded by opposition and had significant impression on the judges about the present scenario.

CONCLUSION

Now to conclude we can say that these kind of cases create a conflict of laws as there is involvement of private international laws as well. These kind of laws involve the laws of two or more countries. If there is so much of chaos in determining the jurisdiction to be applied to such cases, it becomes even more difficult in resolving them.

The shortcoming of law exposed- the initiative taken by law makers to let the technology grow at first and then impose laws on it to curb its growth has created so much of lawlessness and conflicts that it is perhaps difficult to even keep a track on them. More over the knowledge of the absence of laws by a particular section of the society has led to its abuse without any remedy meted out to those who are victimised.

The concept of active and passive defence must be given an impetus. internal use of various technologies and products, such as firewalls and cryptography, and procedures to protect the assets owned by an individual or organization. Some forms of passive defence may be dynamic, e.g. stopping

[32] Poland bows to Sikh demands Available at: http://awazeqaum.com/world-news/12-poland-airport-security-discrimination-against-sikh-turban-lawsuit-part-ii.html accessed on 16th August 2013

an attack in progress by closing vulnerability in real time. But, by definition, passive defence does not impose serious risk or penalty on the attacker. With only passive defensive measures, the attacker is free to continue to assault the target. Given the vulnerabilities of most cyber systems and the low cost of most attacks, a skilled and determined attacker is likely to eventually succeed if he can keep trying safely. Active defence, in contrast, imposes some risk or penalty on the attacker. Risk or penalty may include identification and exposure, investigation and prosecution, or pre-emptive or counter attacks of various sorts.[33]

India, also is signatories to various conventions that were formed pre and post 9/11 attacks in order to ensure a safe and hassle free journey of its citizens, so did many other countries. some of the conventions are: **Warsaw convention, Montreal convention, Chicago convention**. May be, these conventions have been a blessing from many sides but these have also in one way attached shackles on the countries because of which they are also unable to take measures to protest against what they think to be utter violation of some basic rights. Yet the countries have been fast enough in providing remedies to such issues and now there is a requirement of implementation of strict laws regarding the implementation of technologies. Regarding the use of technologies, it is very difficult to create such a system that would be free of all sorts of attacks. When it comes to laws in these arena, there should be uniformity of law for all countries. No country should be prioritised on any basis and given any form of leverages because we must remember that threats do not come in particular shape and size nor with any hallmark. All countries signing to such deal must adhere to it so that none of them raise any question regarding the violation of any law that is in force in their territory. If technologies can be replaced, laws can also be formed and repealed.

The main problem lies herein. Privacy is subjective and variable. So to adhere to a uniform rule-book might become a herculean task to achieve.

Though there should be these minimal layers of protection provided to such systems at the airports- Better firewall, Input sanitation, SQL encryption, Cookie authentication, Http headers usage. Input sanitation checks that only required values type are given as input. So that attacker can't inject in malicious codes that would hack the database. Cookie authentication to verify the user accessing an account.SSL encryption is to establish a secured connection. When inputting username and password one must check if the incoming data to the server is from their own page or not. CSRF protection, Secured socket layer must be used to establish a secured connection between server and client. TSA officials must be given a stricter rules regarding their conduct and mode of operation at such centres.

[33] Network security: Protecting our critical infrastructures, Professor Seymour E. Goodman, Pam Hassebroek, and Professor Hans Klein,Georgia Institute of Technology (United States)

Many times despite the refusal of a passenger to be frisked and the pleas of leaving a flight is turned down, that should be stopped because the personal decisions of an individual must be respected.

India's apex security body the National Security Council admits that India's Cyber security strength is "*grossly inadequate to handle cyber security activities in a meaningful and effective manner*". Therefore ,"now, India is also setting up its own 'cyber security architecture' that will comprise the National Cyber Coordination Centre(NCCC),the Cyber Operation Centre, and National Critical Information Infrastructure Protection Centre(NCIIPC).[34]

The government should start looking for implementation of better technologies that have greatly reduced risks of intrusion to privacy. It is high time that the law makers get ahead and start introducing laws parallel to the introduction of technology rather than wait for the technology to extent itself to its zenith and then try in vain to put to check its venomous tentacles that by the time has already infiltrated the basic structure of a set up. Any country that is setting up electronic and technological measures be it for their security or other forms of protection must keep it in mind that Compromising an individual's data might affect that only person but when the personal data of many individuals are involved there is potential for all kinds of use of data for corporate gain or for misuse for profiling people on the basis of caste, religion, language etc. This would be an unmitigated national disaster not merely because of loss of security and the resulting disgrace, but also because it will effectively allow foreign control of a country's flagship database.[35]

[34] S G vombatkere, 'cyber security, surveillance and democracy', Mainstream, (june 28-july 4th) (2013) at 5

[35] *Id*