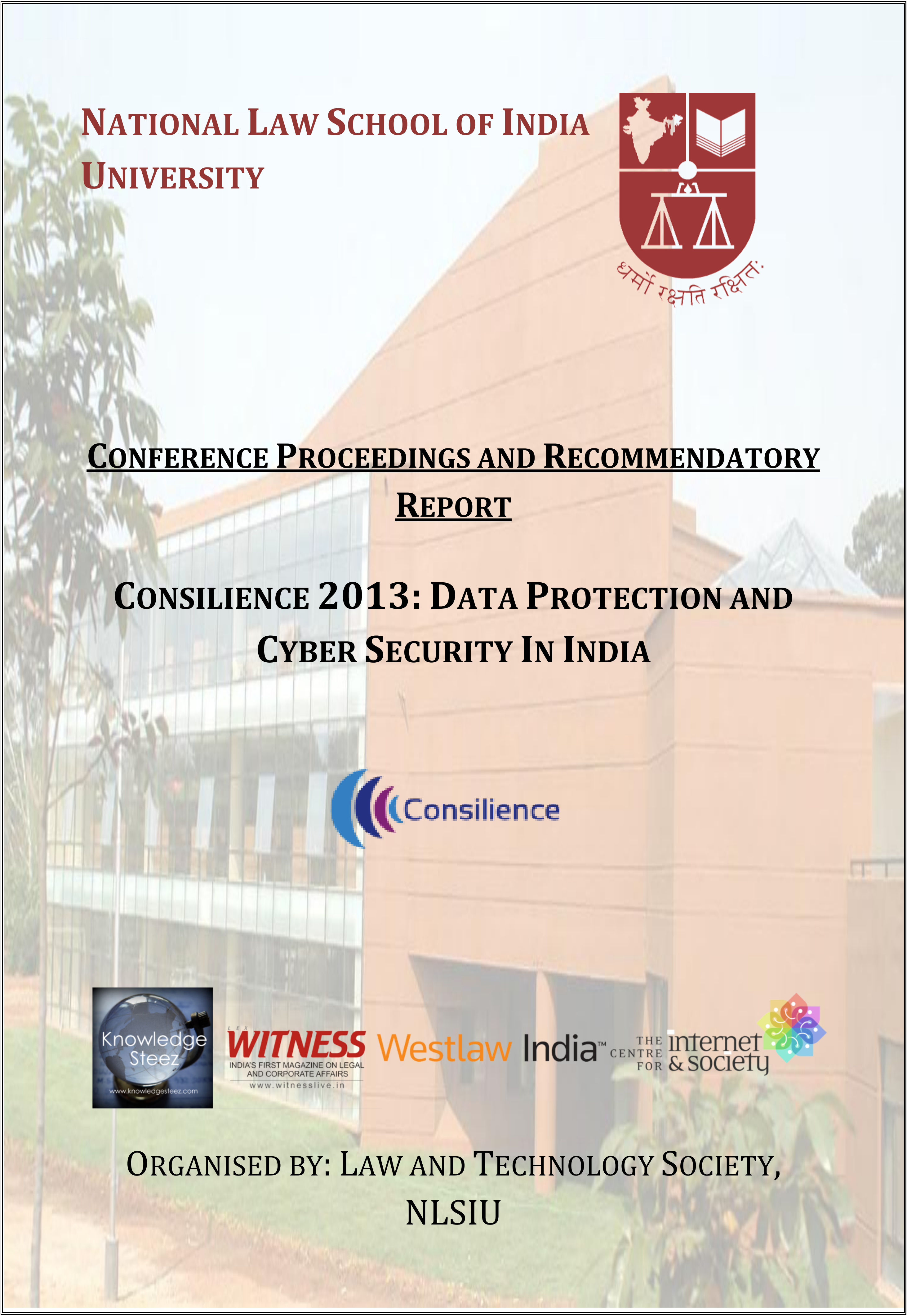

# NATIONAL LAW SCHOOL OF INDIA UNIVERSITY

## CONFERENCE PROCEEDINGS AND RECOMMENDATORY REPORT

# CONSILIENCE 2013: DATA PROTECTION AND CYBER SECURITY IN INDIA

ORGANISED BY: LAW AND TECHNOLOGY SOCIETY, NLSIU

# RECOMMENDATORY REPORT

# SUGGESTIONS ON DATA PROTECTION AND CYBER SECURITY LAWS IN INDIA

## INTRODUCTION

The issue of data protection and cyber security is one which concerns an increasingly large number of persons, through the growing reliance on computer resources. This creates a stronger need for improved protections to individual users as well as companies, governments, etc. Although there are currently laws in place concerned with cyber security and data protection, they are not all-encompassing or necessarily with contemporary relevance. As a result, addressing the lacunae is imperative.

The Law and Technology Society at National Law School of India University, Bangalore functions with the objective of addressing important issues concerning the interface of law and technology. Thus, in its annual conference 'Consilience', it invited the opinions of eminent personalities on the topic of Data Protection and Cyber Security. These opinions, accompanied by the research of a group of students, have brought about the following set of recommendations.

## OVERVIEW OF THE RECOMMENDATIONS

The recommendations have been laid out under three sections.

- **Section I** deals with the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ["Data Privacy Rules, 2011"]. It focuses on the following issues:
  - There is a wide gap between protections extended to sensitive personal data and ordinary personal information, which should be reduced by more equitable protections to both types.
  - An inexhaustive list of conditions for sensitive personal data.
  - Protection of racial, ethnical and political personal information as sensitive in nature.

  - Clearly defined distinction between the data transfer and disclosure to avoid confusion.

- **Section II** pertains to the Draft Privacy Bill of 2010 and suggestions regarding the same, which are briefly as follows:
  - Formation of a distinct authority for trial and adjudication of data protection cases.
  - More qualified provisions and specific phrasing in the exceptions to the right to privacy contained in Section 4.
- **Section III** concerns the National Policy on Cyber Security 2013.
  - Distinguishing between the concepts and scope of cybercrimes and national cyber security.
  - Establishing safeguards to the right of privacy against violations due to excesses by governmental agencies.
  - Clarity on the role and functions of the nodal coordination agency for cyber security.
  - Removal of the policy allowing the use of only unaided indigenous manufactured ICT products.
  - Formation of offensive and risk preparedness strategies for combating threats to cyber security.
  - Regulation of security standards of government agencies.
  - Evolution of industry specific regulations for cyber security measures.
  - Mandatory and incentivised implementation of security standards
  - Cooperation with other nations and engagement with private entities.
  - Incentivising human resource development.

## SECTION I- INFORMATION TECHNOLOGY (REASONABLE SECURITY PRACTICES AND PROCEDURES AND SENSITIVE PERSONAL DATA OR INFORMATION) RULES, 2011

The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 [“Data Privacy Rules, 2011”] is one of the most comprehensive pieces of legislation governing data protection in India. These rules incorporate most of the major internationally recognized data protection principles such as the ones relating to notice,[1] consent,[2] collection and use limitation,[3] access,[4] openness,[5]

[1] Rule 5(3), Data Privacy Rules, 2011.

[2] Rule 5(1), Data Privacy Rules, 2011.

disclosure[6] and safety[7] and hence, deserve appreciation on this front. However, these rules also appear to suffer from certain lacunae, regarding which we offer our opinion in the following section.

## NEGLIGIBLE PROTECTION FOR PERSONAL INFORMATION

The Data Privacy Rules, 2011 differentiate between Personal Information and Sensitive Personal Data or Information. Personal Information has been defined by the Rules as "*any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person.*"[8] Sensitive Personal Data or Information, which is a subset of personal information, consists of data relating to one's financial details such as bank account, credit card, debit card, etc; password; physical, physiological and mental health condition; sexual orientation; medical records and history; biometric information; etc.[9]

While it can be seen that the rules provide ample protection for sensitive personal data or information, they provide very minimal protection for personal information. In other words, information which can be used for identifying a person such as mobile number, name, date of birth, email-id etc. does not figure on the priority list of the government. For instance, the consent requirement and disclosure requirements[10] apply only to sensitive personal data or information and not personal information.[11] So a company might disclose such personal information to a third party if it finds that it is in its interest. For example, the privacy policy of an investment management company reads as "*We may share your Personal Information and transaction history/details with one or more financial advisors/our affiliates/associates who provide or intend to provide services to you or send information to you relating to their products and services.*"[12]

[3] Rules 5(2) and 5(5), Data Privacy Rules, 2011.
[4] Rule 5(6) Data Privacy Rules, 2011.
[5] Rule 4(1), Data Privacy Rules, 2011.
[6] Rule 6, Data Privacy Rules, 2011.
[7] Rule 8, Data Privacy Rules, 2011.
[8] Rule 2(1)(i), Data Privacy Rules, 2011.
[9] Rule 3, Data Privacy, 2011.
[10] Rule 6, Data Privacy Rules, 2011.
[11] Rule 5, Data Privacy Rules, 2011.
[12] BOI AXA Investment Managers Private Limited, *BOI AXA | Privacy Policy*, available at http://www.boiaxa-im.com/footer/privacypolicy.php (Last visited on 10 November, 2012).

### INEXHAUSTIVE LIST OF SENSITIVE PERSONAL DATA

The UK Data Protection Act, 1998 defines sensitive personal data in a comprehensive manner. It consists of information pertaining to:[13]

i) the racial or ethnic origin of the data subject,

ii) his political opinions,

iii) his religious beliefs or other beliefs of a similar nature,

iv) whether he is a member of a trade union (within the meaning of the M1TradeUnion and Labour Relations (Consolidation) Act 1992),

v) his physical or mental health or condition,

vi) his sexual life,

vii) the commission or alleged commission by him of any offence, or

viii) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

It provides ample protection for personal data. In case of sensitive personal data, it just sets more stringent criteria for its safety. For instance, in order to process personal data one needs to fulfil at least one of a certain set of conditions, whereas for processing sensitive personal data one needs to fulfil at least one of another set of conditions in addition to fulfilling one of the conditions for personal data.[14]

In a similar manner, the Indian law can attempt to follow a similar method and thus make the definition of sensitive data more flexible and relevant to the various situations where it may be required to apply.

Though sensitive personal data or information as per the rules consists of a large variety of personal information about the provider of information, certain information is still left out. There have been recommendations of including information related to one's caste,[15] religion,[16] electronic communication records (such as emails and chat logs),[17] political

[13] Section 2, Data Protection Act, 1998.

[14] Schedule 1, Principle 1, Data Protection Act, 1998.

[15] Prashant Iyengar, *CIS Para-wise Comments on Draft Reasonable Security Practices Rules, 2011*, available at http://cis-india.org/internet-governance/front-page/blog/security-practices-rules (Last visited on 10 November, 2012)

[16] Id.

[17] Id.

affiliations,[18] membership of organisations,[19] etc. in the list of sensitive personal data or information.

Inclusion of information such as racial or ethnic origins including caste, political affiliations and religious beliefs is all the more required in a country such as India which is still heavily divided on caste and religious lines. Reports of violence against dalits[20] and religious minorities[21] are not unfounded. Therefore, we suggest the inclusion of this information within the ambit of sensitive personal data so as to protect such communities.

### SIGNIFICANT NUMBER OF EXCEPTIONS TO THE RULES

On 24 August, 2011, the Ministry of Communication and Information Technology issued a press note clarifying that the rules applied only to body corporates located within India. This means that a body corporate located in foreign territory but providing service to Indian citizens can bypass the consent[22] and disclosure[23] requirements as set out in the data privacy rules.[24]

Another exception to rules 5 and 6 laid down in the press note was a "*body corporate providing services relating to collection, storage, dealing or handling of sensitive personal data or information under contractual obligation with any legal entity located within or outside India*". This means that a body corporate which comes into possession of sensitive personal data or information under a contract with another legal entity is not subject to the rules 5 and 6. For example, a company A collects information about a person X complying fully with the data privacy rules. However, if company B comes into possession of such information about X through a contract with A, it (B) is not required to follow the data privacy rules.

[18] Apar Gupta, Comments on Draft Sensitive Personal Information Rules , available at http://www.iltb.net/2011/02/comments-on-reasonable-security-practices-and-procedures-and-sensitive-personal-information-draft-rules-2011/ (Last visited on 10 November, 2012)

[19] Id.

[20] Lyla Bavadam, *Dalit blood on village square*, FRONTLINE, (November 18, 2006), *available at* http://www.frontlineonnet.com/fl2323/stories/20061201004713000.htm (Last visited on 10 November, 2012).

[21] Krittivas Mukherjee, *Christians cower from Hindu Backlash in Orissa*, REUTERS, (September 3, 2008) available at http://in.reuters.com/article/2008/09/03/idINIndia-35291320080903 (Last visited on 10 November, 2012)

[22] Rule 5, Data Privacy Rules, 2011.

[23] Rule 6, Data Privacy Rules, 2011.

[24] *Clarification on Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 Under Section 43A of the Information Technology ACT, 2000*, available at http://pib.nic.in/newsite/erelease.aspx?relid=74990 (Last visited on 10 November, 2012).

### OVERLAP BETWEEN DISCLOSURE AND TRANSFER REQUIREMENTS

Rule 6 of the data privacy rules deals with disclosure requirements and rule 7 deals with transfer requirements. However, the difference between the two terms (disclosure and transfer) has not been spelt out clearly in the data privacy rules.

The difference is vital since the rules dealing with disclosure and transfer specify different requirements for each of them. For instance, to disclose sensitive personal data or information to a third party, the body corporate does not need to ensure that the third party affords the same level of data protection as itself, whereas to transfer such information, this requirement has to be fulfilled.[25] Therefore, a company A might disclose sensitive personal data or information about a person X to a third party B that does not ensure the same level of data protection as A by justifying such act under Rule 6 dealing with disclosure.

We thus suggest that difference between Rule 6 and 7 is more clearly fleshed out, so as to avoid any confusion regarding which conditions would apply to a particular situation.

[25] Raghunath Ananthapur, *India's New Data Protection Legislation,* 8(2), SCRIPTED 193, 200 (2011).

## SECTION II- DRAFT PRIVACY BILL, 2010

The following section of the report focuses upon the important issues which need to be addressed by any privacy legislation and institutional regulations, with reference suggestions in the AP Shah Privacy Report read with the Draft Bill.

### JUSTIFICATION FOR A SEPARATE DATA PROTECTION AUTHORITY:

Section 49 of the Privacy Bill enables the creation of a separate data protection authority which handles administrative responsibilities. Adjudicatory responsibilities are handled by the Cyber Appellate Tribunal (CAT) as constituted under Sec. 48(1) of the IT Act, 2008. However, at present the Tribunal may not be a body capable of handling the logistical difficulties of being the trial court for data protection cases, in lieu of the fact that it currently functions as an appellate court.

Therefore, there is the alternative possibility of giving the Data Protection authority the limited role as the adjudicator of disputes, while making the CAT the court of first appeal, and establishing branches of this authority in each of the states. Though Sec. 58 of the Privacy Bill does give some adjudicatory powers to the Data Authority, its relationship with the CAT is not clearly defined.

Alternatively, and in consideration of the fact that the body is elected by and thus not independent of the Central government, adjudicatory powers over privacy disputes can be given to the judiciary.

### SCOPE FOR MISUSE OF EXCEPTIONS:

Section 4 of the Bill discusses the circumstances in which privacy rights of individuals can be breached. Among other things, privacy can be invaded for the prevention of the incitement of any offence, for friendly relations between states, for the prevention of public disorder or the detection of crime, and for the protection of rights and freedoms of others. These provisions are vague enough that most infringements on privacy can be justified, therefore defeating the purpose of the legislation itself. For example, it may be used to provide personal data of harmless users of a mailing service to another country that has requested the same and regardless of whether there exists a serious allegation against these users. This can all be done for the purpose of friendly relations with this foreign state.

Thus, this provision requires either specific guidelines to its exercise or stringent supervision of its application. Moreover the first provision of Section 4 allows for infringement of privacy for the sovereignty, integrity and security of India, which makes provisions 2 and 3 redundant. It would be advisable to develop a list of offences for which it will apply. Further, there must be a clear nexus between the crime and the method used for detection, so that there is no excessive access to personal data.

Therefore it is recommended that these provisions are made more specific in nature. The Privacy Protection Bill as drafted by the Centre for Internet and Society proposes a system in which prior authorization is required from a Chief Intelligence Officer under clearly defined conditions. But a transparent appointment process is required to be taken to ensure that the autonomy of these officers is guaranteed.

## SECTION III- NATIONAL POLICY ON CYBER SECURITY 2013

Specific sections of the National Policy on Cyber Security 2013 [“the Policy”] on which recommendations are given, are discussed below.

### PREAMBLE - PARAGRAPH 5

*Definition of Cyber Security*

This paragraph broadly identifies the threats the Policy wishes to address. However, all these threats need to be distinguished from those that endanger cyber security. What the policy describes as incidents of “national significance” leading to damage to lives, economy and national security”, such as cyber terrorism, cyber warfare and breach of government secrets are clearly matters of cyber security.

However, issues of identity theft, phishing, hactivism and the like pose a threat to individuals and not, strictly, to the national security. These are matters of cyber crime. The Policy should necessarily differentiate the two as the mechanism to address both is different. For example, the Central Monitoring System (CMS) has been justified, compromising privacy rights, on the basis of protecting cyber security. If an additional range of threats (cyber crime) are included with this fold, the justification will not stand as these crimes are not as grave as those threatening national security.

Moreover, there are a number of agencies and institutions already in place. Differentiating between the two types of risks will help dividing the responsibilities of these agencies and the level of power and resources that can be granted to these agencies.

### III Objective (10) – Data Protection and Privacy

While this has rightly been identified as an objective of the policy, the strategies listed in Section IV do not directly deal with this issue. Since surveillance mechanisms and the Central Monitoring System exist, there need to be safeguards and guidelines to protect citizen's privacy against excesses by law enforcement agencies. Reference can be made to the Privacy Bill as a standard against which to test the actions of government agencies apart from the cyber criminals infringing on privacy of citizens.

### IV A – Creating a Secure Cyber Eco System

#### *IV A (1) - Designation Of A Nodal Agency To Co-Ordinate All Cyber Security Matters*

More clarity is required on this nodal agency. Here, the distinction between cyber security and crime becomes significant as it needs to be determined whether this agency should restrict itself to matters of national significance, or cyber crime as well. Additionally, it is unclear what the position of this body is, in relation to CERT-In which is designated a nodal agency for cyber security emergency response and crisis management in IV E (2) and in relation to NCIIPC which is designated a nodal agency for critical infrastructure information protection in IV G (2). The responsibilities and hierarchy of each should be enunciated.

#### *IV A (8) – Procurement Of Indigenously Manufactured ICT Products*

This section seems to suggest that indigenously manufactured ICT products will be mandated to be procured to the exclusion of imported ICT products. Such a regulation can prove counter-productive. This is because it not possible to ensure that the best technology and developments will necessarily be independently developed by indigenous manufacturers. Further, the type of cyber risks change rapidly requiring constant innovation, something that the country will have better access to if the international market is considered as well.

While it is true that imported products may increase vulnerability, this can be combated by verification through free and open-sourced software (FOSS) which provides security through transparency where users can themselves identify malware or bugs, endorsed by Strategy IV C of the Policy. In addition, source code escrow agreements also work as a verification measure. Recently, the Indian government used just such an agreement to procure from Huawei and lift the ban on their products which was imposed due to the severe security breach. This can ensure technology neutrality while maintaining cyber security.

### *IV-D – Strengthening Regulatory Framework*

This section lays down the need for a more robust legal framework. It is recommended that the procedural aspect of law be emphasised. The nature of cyber threats and crimes are such that the existing procedural and evidence appreciation laws are inadequate. Issues of effective seizure of storage media, jurisdiction of courts and police, legality of surveillance mechanism, disclosure of path of packets by ISPs and other investigative techniques and evidence collection techniques need to be highlighted and addressed. This is in keeping with Objective 11 of the Policy.

## IV E – SECURITY THREAT, VULNERABILITY MANAGEMENT AND RESPONSE TO SECURITY THREATS

### *Offensive Strategy Required*

This section, along with the Policy as a whole, aims to improve the defence of the nation against cyber warfare but does not focus on preparation for offensive cyber action as well. As per Article 51 of the UN Charter, a country may engage in self defence tactics in the face of an attack. In the context of the cyber warfare, this right cannot be effectively availed of, if the nation lacks the technological capacity and offensive strategy.

The various methods of cyber warfare such as espionage (such as *Titan Rain* and *Moonlight Maze*), vandalism and sabotage should be clearly identified and defence along with counter measures should be developed, identifying appropriate authorities (RAW, DRDO) to formulate and implement such strategy. The Policy can envisage the establishment of CERTs or CERT like authorities in the Army, Navy, Air Force and Intelligence Organisations.

Further, the Policy should encourage the formation of specialised cyber warfare units similar to existing conventional warfare units and Territorial Army Battalions for the Railways and Oil and National Gas Corporation. Such units can be composed of IT experts who can be deployed during times of increased threats such as the Commonwealth Games during which there were cyber attacks on critical networks.

### *Measurement Of Risk And Preparedness*

In addition to the strategy mentioned, there is a need for the evolution of a standard mechanism for testing preparedness and risk management against cyber attacks of both government and private bodies. This mechanism should be deployed regularly through announced and unannounced checks in order to thoroughly ensure risk mitigation. This can be carried out by the Information Technology security auditors already appointed by CERT-In.

### IV F – Securing E-Governance Services

Since, crucial areas such as defence and defence related research and development, space, energy and law enforcement are increasingly relying on internet based services and mobile storage, Public Key Infrastructure (PKI) should not only be encouraged but mandated to ensure secure communication. This is crucial to tackle cyber terrorism and cyber warfare. The success of the National e-governance Program is dependent on such security. Further, all government agencies should be mandated to comply with existing security standards such as DSCI Security Framework.

### IV G – Protection and Resilience of CIIs

#### *Evolution Of Industry Specific Regulations*

Several critical infrastructure industries such telecomm including undersea cables, stock exchanges and electricity are handled by private entities. Each sector utilises different types of technology and is, thus, vulnerable to different types of attacks. Thus, regulation and best practices with respect to cyber security differ from industry to industry. For example, the United States has enacted separate cyber security regulations for Health Insurance and Accountability and Financial Services (Gramm-Leach-Bliley Act). Such an approach is required in India as well. In fact, several other industries such as software manufacturing, ISPs and industries that regularly deal with private information of citizens should be provided with industry specific regulations. The Policy should aim to encourage such legislation.

#### *IV G (2) – NCIIPC*

As earlier discussed, this body's position with respect to the nodal agency mentioned in IV A (1) is unclear. An earlier draft Policy, the NCIIPC was to function under the existing National Technical Research Organization (NTRO). In this Policy, however, the body's functioning with respect to each other is not mentioned. Further, the role of the Ministry of Defence and the Ministry of Home Affairs, both of which concern themselves with matters of cyber security in relation to this nodal agency is unclear. If this nodal agency is to be constituted of representatives of these ministries, this should be made clear.

Further, the responsibility and functions of the Central Monitoring System, Data Security Council of India (DSCI) and the National Skills Registry is not mentioned at all in the Policy. Some light should be thrown on the role of these bodies.

*IV G (4) – Mandatory Implementation Of Global Best Security Practices In CII*

This can be accompanied by financial incentives such as tax deductions and rebates on investments on cyber security, loans for them, etc. This is in keeping with Objective 9 of the Policy. Further, the liability of the CII operator in case of breach of security guidelines needs to be elaborated upon.

### IV M – INFORMATION SHARING AND COOPERATION

*Co-Operation With Other Nations*

The Policy mentions the importance of co-ordinating efforts to tackle cyber threats with other nations. However, another important aspect is the need for India to engage in international dialogue on the development of international law regarding cyber threats. While no overarching international convention on the matter exists, its formation is underway. In this situation, India needs to form a definite stance to ensure that the treaties to come are not skewed in favour of internationally powerful nations and maintain the national interest of India with the help of the Joint Committee on International Cooperation and Advocacy. For example, Russia has maintained a strong argument against Article 32 of the European Convention on Cyber Crime as undermining its sovereignty.

In addition, an institution or agency or a facet of an existing agency should be identified by the Policy as one that should maintain constant contact with corresponding authorities of other nations for seamless information exchange.

*Co-Operation With Private Entities*

The Policy should envisage the setting up of Information Sharing and Analysis Centres as recommended by the Joint Working Group on Engagement with Public Sector on Cyber Security, within private sector enterprises that are mandated to co-ordinate with CERTs and provide them with necessary information and report all cyber attacks. As of now, only the

Intermediary Guidelines require intermediaries to report cyber attacks to the CERT-In. The Policy should envisage such a disclosure requirement across all private sector enterprises.

More importantly, it is seen that private enterprises face liability on sharing private information of clients, especially in international proceedings. In order to encourage information exchange with these enterprises, legal changes and exemptions have to be made while ensuring strict compliance with guidelines protecting privacy.

Another measure that should be included in the Policy is the mandatory appointment of a Chief Information Security Officer similar to an auditor in all private and government bodies who can ensure compliance with the regulatory framework and help in the information relay process. So far, only the banking sector has this as a mandatory requirement.

### IV J – Human Resource Development

One of the ways to develop human resources in the march against cyber threats is to conduct prestigious talent spot competitions such as CyberPatriot. These would incentivise the efforts against such threats and allow for building of skills and general awareness of the issues being combated.

# CONFERENCE PROCEEDINGS

## DATA PROTECTION AND CYBER SECURITY IN INDIA

### DAY 1-MAY 25, 2013: CYBER SECURITY

### SESSION I: CYBER SECURITY IN INDIA: WHAT IS THE CURRENT SCENARIO?

*Amid the spying saga that unfolded in 2013 coupled with recurrent news reports of intrusive measures by the State over citizens' personal data, the government indicated its attempts to draft the National Cyber Security Policy. The concerns are two-fold: firstly, protecting the private and public infrastructure from cyber attacks from inside and outside forces, and secondly, safeguarding the user's personal and financial information from all persons, including the government's very own. The issue of cyber security assumes importance not only in terms of India's own institutional framework, but also to clarify India's stand in the international community, which has been sceptical of India's cyber defences. The ideal normative framework of such a Policy in the Indian context needs to be discussed as there is undoubtedly a pressing need for regulation on this long-neglected issue.*

The first session of Consilience - 2013 successfully commenced with Jasraj Singh, Convenor of the Law and Technology Committee, NLSIU introducing the event, with a short speech on the origin of the conference and the subjects it has focused on over the years. Thereafter, Professor T.V, Subba Rao, Chairperson of the Undergraduate Council, NLSIU gave the inaugural address where he welcomed the Chief Guest, Justice S.R. Bannurmath, former Chief Justice of the Kerala High Court, as well as the other panellists – N.S. Nappinai (the founder of Technology Law Forum), Naavi Vijayashankar (founder of portalnavi.org), Dr.Samir Kelekar (who runs a technology consultancy firm) and the moderator, Manojna Yeluri. Professor Rao congratulated the Law and Technology Committee on the successful organisation of the conference and stressed upon the relevance of the topic of cyber security in India, as well as the problem of 'lethargic legislative response' that the concept faced.

The keynote address was delivered by **Justice Bannurmath** who headed the Committee for computerisation of the court system in Karnataka. While explaining the importance of technology in everyone's lives, he took care to stress upon how the positive impact of cyber-usage was being overshadowed by the evil effects of the same, one of the major threats being in the form of cyber-security. Of the many cyber crimes prevalent in India, the most commonly seen are occasions of hacking (by agencies operating in China), cyber stalking, bank account frauds etc. He also said that a major hindrance in prosecuting such crimes is that the perpetrators are ‘faceless’, i.e. they are anonymous. The discussion in the session basically revolved around the issues of cyber security and devising ways to prevent oneself from being a victim of such crimes. Another problem that was pointed out by him was the ‘boundary-less’ nature of cyber crimes, and he emphasised on the requirement to make laws which were tailored to the needs of the stakeholders. Along similar lines, the moderator, Ms. Yelluri, said that the two biggest concerns today are data protection and cyber security.

The first session of Consilience 2013 is based upon the broad theme of cyber security in India. The discussion by a panel of three speakers is led by Ms Manojna Yeluri.

**Ms. N.S. Nappinai:** In the wake of increasing concerns on cyber security, Ms. Nappinai said that the world has changed from being relatively safe to being extremely danger-prone. Thus, even the cyber world needed security measures, especially since important public institutions like the Railways, the Nuclear Corporation of India and others face up to 10 cyber attacks per day. Children are at a greater risk because of an extensive use of social networking sites. Other threats faced by individuals are in the form of stalking, identity theft etc. She advocated the use of law as a tool for deterrence.

She thereafter listed out the cyber security measures that have been taken in India, explaining the origins of Indian Computer Emergency Response Team (that began in 2004), and National Critical Information Infrastructure Protection Centre (NCIIPC), amendments made to the Information Technology (IT) Act. However, she argued that these measures have been ineffective in reducing cyber crime due to lack of reportage of cyber crime instances as well as the laggard criminal justice system in India, which dissuades people from approaching it. The major concern that India is currently grappling with, in the context of cyber security, is misuse of IT provisions vis-à-vis their utility and the question of privileging greater number of amendments over better interpretation and implementation. She concluded that while the State and industries can still protect themselves, there is a need to protect individuals as they are helpless against the misuse of cyberspace.

**Mr. Naavi Vijayashankar:** Mr. Vijayashankar focused on the process of victimization, which is on the rise, owing to lack of awareness on the requirements of cyber security. He contended that law must be created in such a manner that this ignorance of the people is factored in.

He analysed the launch of AADHAR number, which he believed is prone to misuse because of its large database of biometrics and sensitive personal information. Mr. Naavi specifically raised the point of regulating the ethical hacking training sector, which currently is not governed by any laws, but can easily be a breeding ground for cyber criminals. He suggested some solutions to curb cyber crime, in terms of setting security goals that India needs to focus on. Some of the suggested goals were prevention of breaches by spreading knowledge of cyber security, building a culture of security, fortification of intelligence-gathering and defence, requirement of surveillance with sufficient safeguards, building deterrence through law, quick prosecution of criminals, setting up of a Cyber Security Coordination Centre, etc. He indicated how the role of such a Centre will be different from that of CERT-In and how it will coordinate with NTRO, CBI  and other such agencies. Despite the presence of legal infrastructure to combat cyber crimes, adjudication officers and Cyber Appellate Tribunal have been under-utilised. Further, he discussed the police infrastructure that supports this legal framework, such as the draconian powers under the IT Act, as well as the shortage of manpower that the country faces today with respect to cyber security professionals. The solution suggested by him is that the citizens should take control to protect themselves online through a ‘Netizen Protection Forum’. He also encouraged the NLSIU community to act as a catalyst in this regard, beginning with the formation of a pressure group to force the country into revising its existing cyber security systems.

**Dr.Samir Kelekar** Dr. Kelekar also expressed the concern over inability of law to keep pace with the technological growth. He explained the sort of problems he himself had faced as a technology consultant to the state of Goa for teaching people the use of cyberspace, and the sort of negligence the management of these aspects faced.  He explained the problems of using RR number in paying electricity bills which can easily be misused by anyone. He also discussed the disadvantages of implementing the AADHAR system, echoing Mr. Naavi’s thoughts. He drew attention towards the negligence of state authorities in protecting the netizens of India. He cited examples of the repeated use of Huawei and ZTE modems/routers even though they have been repeatedly found to be problematic owing to links with the Chinese government.

**Student Presentation: Udbhav Tiwari**

Udbhav Tiwari, a student of IInd Year, WBNUJS Kolkata presented his paper called 'Cyber Security: Policies and Perspectives' at the session. Mr. Tiwari analysed the rise of the National Informatics Centre in India around the year 1978, and thereafter the Ministry of Information and Technology under the Ministry of Broadcasting in the 1990s. He attributed their inefficiencies to the bureaucratic process of appointment and lethargy in new policy devising approaches. Further, he explained how the IT Act did not change things in any way and cited the example of India's condition during the Y2K virus crisis, wherein the level of awareness and expertise was so low that consultants from abroad had to be called to help Indian authorities and companies. Thereafter, India began taking baby steps by establishing CERT-In, based on the U.S. model for focusing on the commercial aspects of cyber security measures like protection against hacking and cyber attacks. Explaining the functions of the National Critical Information Infrastructure Protection Centre (NCIIPC) in defending critical national infrastructure such as nuclear power plants and defence infrastructure, he outlined its failures as well. Some of the failures included daily defacement of government websites and theft of sensitive information. The biggest problem in combating these is that most of the people tend to characterise these attacks as 'Chinese' or 'Pakistani' infiltrations and therefore seek solutions through diplomacy, instead of trying to improve the cyber security framework. Mr. Tiwari listed out the other reasons for India's failure in protecting itself- such as lack of funding, nascent cyber culture, absence of nodal agencies and the omnipresent lack of awareness. He finally concluded his presentation by analysing the Draft Cyber Policy of the Government of India 2013, which aims to strengthen the cyber security network, provide a secure computing environment and build cyber security intelligence.

Signalling the end of the first session, Ms. Yelluri, the moderator summarised the discussion of all speakers and highlighted the government's lack of sense of direction in pursuing a way to protect the cyberspace. Finally, the session concluded with several questions being raised from the audience. One of the questions raised was regarding the extent to which international guidelines played a role in cyber security in India. In response, Dr. Kelekar asserted that while there were firms to certify that companies were following these guidelines, most could avoid compliance by paying money to these firms. Another important question asked by a member of the audience was with respect to the utility of the AADHAR number. Dr. Kelkar, however, disputed this by pointing out its disadvantages.

## SPECIAL ADDRESS BY VIKRAM ASNANI (FROM THE DATA SECURITY COUNCIL OF INDIA)

Mr. Asnani began by pointing out that the first session had taken a gloomy turn. Though he agreed partially with the negative points put up before him, he believed that there were positive points as well. In his opinion, it was not fair to compare US with India as they were a much more matured country on this front. He highlighted that Indian organisations had been active in learning from the US.

He then went on to talk about the large scale nature of the Unique Identification Authority of India (UIDAI) project. He said it was obvious to have some glitches in a large project. To support his point, he gave the example of The Pentagon which was hacked even though it had world-class facilities. Hence, the Indian websites cannot be blamed.

He admitted that AADHAR did have a political angle as it was required for the government's schemes. He did agree that there are problems of biometric data. But he stated that the very concept was a wonderful thought. According to him, the problem of AADHAR and National Population Register (NPR) will take time as immediate work was difficult in the light of prevailing circumstances.

He then moved on to discuss the topic of cyber security. He said that global data flows cannot be curtailed, especially with cloud data which provides no clue as to its location and storage. Even US is struggling with the same, he commented. Cyber-crimes earlier were about monetary things. It was difficult to find what was stolen, unlike a physical theft. However, cyber criminals are now very innovative. Knowledge about penetrating into secured sytems had also dramatically increased.

He highlighted that as a country, India has worked a lot. The government has reached 3.2 lakh students in terms of basic internet awareness. The requirement now is to work hard to operationalize the system. With a brief round of questions from the audience, his talk came to an end.

## SESSION II: THE DRAFT NATIONAL CYBER SECURITY POLICY: WILL IT BE SUFFICIENT?

*The absence of a cyber security framework is an often-criticised aspect of India's cyberspace infrastructure, and has received attention at the national as well as the international fora. With the heightened awareness of cyber-threats, the Draft National Cyber Security Policy did its rounds on the desks of the interested stakeholders. In this session, the panellists discuss the issues ranging from necessity to the scope and constitutionality of this Draft Policy. Implementation also is a key issue that never fails to trigger discussion, especially in the* *context of weak administrative structure in India. It must be pointed out that some time after the conclusion of this Conference, the National Cyber Security Policy was unveiled by Shri Kapil Sibal, Union Minister for Communications and IT. The government has also acknowledged that the "real problem" lies with the operationalisation of the policy.*

*The third session involves Ms Manojna Yeluri (advocate and legal researcher), Mr Vikram Asnanai (Senior Consultant with Data Security Council of India (DSCI) and Mr Apar Gupta (Advocate, Delhi High Court) as speakers and Ms NS Nappinai (founder of Technology Law Forum) as the moderator.*

The afternoon session began with the venerable moderator *introducing the broad areas that had to be covered in the session. These were identified thus:*

- Do we really need the National Cyber Security Policy?
- What is the intent, purpose and focus behind this?
- What is it really going to achieve?
- Can it do something that the Act itself has not been able to do or is it there to supplement the Act and in what manner?

Thus, the floor opened for various speakers to put forward their views on the aforementioned and other related issues.

**Manojna Yeluri :** Ms Yeluri put forward the reasons which led to bringing about such a policy. Some of the major reasons were - the confusion about legal rules in India, their implementation concerns, and the need for equipping computing policy with better infrastructure. Also, with the advent of such a policy, the international organisations will have more faith in our system. This is necessary because India is becoming globalised. She pointed out that essentially there are 5 mandatory considerations laid down under Para 1 of the Policy:

1. Mandatory issues NEED to be addressed.
2. Need for dynamic, contemporary and effective solution to cyber security threats.
3. Emphasis on cyber security intelligence – to anticipate counter attacks and attribute them to their sources
4. Creation of effective crisis management strategies depending on their significance
5. Building up human and technological infrastructure.

The policy has been drafted with the broader aim to target all kinds of IT users and acknowledges the complexity of cyber threats. Hence, the solutions must be contemporary and dynamic and not confined to the traditional solutions of installing firewalls and virus checks. However, the Policy has not adequately elaborated upon them. A criticised aspect on aforementioned issue (3) is lack of the right infrastructure in India that at times leads to bringing the wrong people to books. Issue (4) has been criticized to have brought in a hierarchy of problems, though unclear.

Para 3.13a lays down some of the security best practices, the implementation of which shall be unprecedented and interesting. These include appointment of Chief Information Security Officers- they are supposed to be contact persons at the high management level and the nodal point for information. The policy envisages two kinds of actions: a) Enabling actions i.e. promotional, advisory functions and b) endorsing actions which are commercial in nature and involving more than one certified service providers.

Some of the aspects of the Draft Policy include:

IT security Product Evaluation: This includes certification and assessment that will certify IT products with respect to international standards.

IT manpower: The policy looks to spreading awareness so that people may avoid having to seek legal remedy. Also there is an urgent need for indigenous R&D – to have sophisticated software, defence systems that will help build faith in the system. Absence of a healthy cyber culture in India is another blot in the face of successful implementation of the policy.

Ms. Yeluri pointed out some of the major the legal issues involved in the policy. There is no mention of Privacy at all. Regulation raises the question as to where should the line demarcating privacy and surveillance be ideally drawn. This is a major challenge in regulation of a free space like cyberspace. Absence of its mention indicates that the policy is actually justifying such invasion which can be a cause of problem in the long run. Hence according to Ms. Yeluri, the policy leaves us with doubts and scepticism.

**Vikram Asnani:** Mr Asnani too elucidated the need for this policy as a measure to repair the flaws in the previous legislations. This policy ensures accountability which IT Act couldn't. Not only the Government, but also private entities are party to it. This is commendable as private users account for 80% total IT users and therefore there has to be a policy that goes overboard to ensure correct usage. The positive aspects of the policy are that it creates capacity building workforce which ensues ethical usage, employment in private and public sectors as well as nodal agencies like the Chief  information Security Officer,. Moreover, it strengthens the regulatory frameworks, facilitates education and creates awareness for public prosecutors. It also creates early warning systems, information sharing and analyses centres (e.g. Banking sectors), crisis management, drills – which he thinks will help build resilience.

However, he too expressed his unhappiness with the policy on account of it not being drafted with proper precision, having only pointers and statements that may only remain policy items. Addressing the question as to whether the ethical and regulatory issues are being intermixed in the policy and whether the policy is more State-centric in disregard of individual privacy rights (eg during hacking), Mr Asnani said that the policy is supplementary to the law and did not tend to overrule it. The IT Act will cover cases of individual hackers and it is under its ambit as breach of a policy is not greater than that of law. On the question as to whether the government is unable to keep pace with the private sector when it is the private sector that generates maximum growth, Mr. Asnani responded by admitting that indeed this is a reactive policy. Technology is moving so fast that even the industry is not keeping up with it.

The moderator's major concern was that the policy seemed to be redundant in the sense that it had come after a series of legislation, starting from the 2000 IT Act. Hence, the policy should have ideally preceded the Act. Ms Yeluri expressed the same concern by saying that if the answer to this dilemma was that the policy is in fact a thought process, then it seemed as if the Act was thoughtless. Col. Mathew (Founder, Citizens Action Forum) from the audience addressed these issues asserting that the IT Act was a control measure whereas the policy had a different purpose of cyber warfare. The Policy was meant to look at the infrastructure, primarily the government infrastructure. The policy hence aims at a different cyberspace altogether as compared to the IT Act, which looks at internet and social media.

**Apar Gupta** Continuing the discussion, Mr Apar Gupta also agreed that the policy is the need of the hour. He said that the 12 govt institutions mentioned in the annexure are critical for the policy. Presently there is no uniformity between government infrastructure and sectoral infrastructure.

The policy suffers from various definitional issues. One thing which is common to all cyber security policies is that they look inward at government, rather than the establishment. In his opinion, the policy does not try to regulate the private sector. The government has not made the important provision of mandating standards for encryption according to 84a. Government has not even notified rules effective for encryption. There is also a need for uniformity amongst the present differing standards applicable to phones, banks, RBI banking regulations and other sectors. Different encryption caps cause a great deal of confusion. Also, the imposition of certification on the private sector seems to lack any legislative basis. It is bad for business and for indigenous companies as they will have to pay to get ISO certification which can affect pricing as well. Such a scheme raises suspicion as to if it is actually a larger scheme to fund certain certification agencies by forcing them to private sectors.

Hence to sum it up, the Policy looks like a solution in search of a problem, but it does help since internet is pervasive. IT act has not been implemented efficiently, tribunals under it have not been created, adjudicators are not competent, and there is a backlog of cases. Thus, there are broader issues to be dealt with.

**Aditi Bakshi (Student Speaker)** Aditi Bakshi, a student from BILS was the student speaker for this session. She initiated her speech by stating that cyber space is beyond territorial context and is a global interconnected sphere. There are 150 million internet users in India. NCSP targets Information and Communication Technology users, service providers, individual users, government and NGOs. The problem with the policy lies in its vagueness and its definitional issues: though there is Critical ICT infrastructure, absence of a comprehensible list will make this impractical. Vague representation as to the target population has been recognised, but no specific guidelines have been laid down.

Also there is no way to inform cyber security breach or incident as many private companies do not report. This is unlike US where companies are forced to declare such incidents.

There is no universal law in the field of cyber space. This also makes cyber crimes difficult to prosecute. There is a need for an apex body that would help remove ambiguities.

Implementation will take many years, and sooner is too idealistic. However there are no immediate measures for the present threats. However, appropriate measures like skills training, removal of obsolete database, adopting risk-based approach and a flexible policy structure can help provide a good defence.

Finally the session concluded with a round of questions from the audience. They have been discussed hereafter. One of the questions was “How can a level of awareness for self-protection, reasonable access control, etc be maintained as what the policy seeks to achieve?" Mr Apar Gupta dismissed its possibility calling it misplaced and being outside its scope. He said a national policy is only concerned with individuals in case their accounts are hacked and information compromised. It is not possible to have one policy for the internet to make a complete clean environment as it's idealistic. Ms Yeluri asserted that it was no new problem as whenever laws are drafted, aims are idealised. However, we can't possibly have one law which fits everyone.

Another question was raised on the issue of legality of mapping of customers without telling them. The panel responded by saying that the same depends upon where they are getting our information. If it is from sources where we voluntary disclose information, then there is not much problem. However, if it is the case like that of Google facilitating the email system, then extracting information from people's private mails would be illegal.

## Session III: Cyber Security and Surveillance: Is surveillance justified for cyber security purposes?

*Often, the backlash against surveillance jeopardises cyber security, or is commonly perceived to do so. Hence, one of the recurrent themes that come up for debate is the balance between the two concepts. The backlash emerges from the concern over privacy rights of individuals. The reports about increasingly intrusive and sophisticated surveillance techniques have only aggravated fears about the real intentions that the State is trying to pursue in the name of cyber security. In this session, the panellists discuss the interlinked concepts of cyber security and surveillance to address the question as to whether surveillance is justified in the name of cyber security.*

*The speakers for the fourth session include Jacob Appelbaum (Core Member, Tor Project and Former Spokesperson, Wikileaks), Hormis Tharakan(ex-chief of the Research and Analysis Wing (RAW)), Saikat Datta (New Delhi Chief of Bureau, DNA Newspaper) and Maria Xynou (Policy Associate on the Privacy Project at the Centre for Internet and Society (CIS)). The session is moderated by Mr. Pranesh Prakash (co-founder, CIS).*

The evening session for the day began with the venerable moderator for the session Mr. *Pranesh Prakash* introducing the topic for discussion i.e. Cyber Security and Surveillance: Is surveillance justified for cyber security purposes? *Mr Prakash his speech suggesting 4 propositions on surveillance:*

1. Making surveillance easy makes us less secure.

Researchers of the Tor Network running an exit note for a few months found that they had access to the communications between embassies and their home countries for many countries. The password (including the password of the ambassador based in Beijing) was published in the Indian Express. Even after that, for a week, the password had not been changed. This happened due to lack of encryption. End to End/person to person encryption is permitted, but bulk encryption is not which makes it possible for everyone to listen.

2. Surveillance is not about security. It is about politics.

Series of fake requests are being accepted by telecom companies resulting in actual surveillance, a case on point being the Amar Singh case. More than 90,000 fake requests are accepted by telecom companies in Gujarat.

3. Current technology doesn't accept existing legal standards on surveillance.
4. Digital arms trade; cyber warfare is emerging as greatest threat.

In order to elaborate on the themes underlined above, the panellists began their discussion.

**Hormis Tharakan:** Mr Tharakan, drawing attention to increasing threats from cyber space, stressed upon the fact that protection for National Security has become the most critical requirement. There is a need to ensure economic security which can only be done through multiple redundant system to counter all types of attacks. He elicited some of the existing methods of cyber attacks which are as follows:

- Physical Attack: Infrastructure may be destroyed and damaged through conventional methods.
- Syntactic attack: Modifying behaviour and logic of the system. Makes the system faulty and un-usable.
- Semantic Attack: data transmitted or saved is modified without knowledge of the user. Most treacherous. Hardest to mitigate.

Motivations for cyber attacks, as pointed out by Mr Tharakan, emerge from various factors such as countries planning to use cyber networks for warfare, collection of intelligence, cyber crime, mischief, terrorism etc. All categories of attackers, be it state or non-state actors are incessantly stepping up their capabilities for attack. This has to be combated.

*History Legislation in India of Cyber-security*

For many years, the only statute governing the use of technology for surveillance purposes was the Indian Telegraph Act of 1885. The IT Act was introduced in 2000. The enactment of the IT (Amendment) Act, 2008 brings India to the league of countries that have a legal regime for cyber security and privacy.

*Emerging Policy Framework*

- Report of the Group of Experts on Privacy, 2012
- Report of the Joint Working Group of National Security Council System on Engagement with Public Sector on Cyber Security.

The other upcoming projects and schemes include: National Counter Terrorism Centre (NCTC), Crime and Criminal Tracking Network and System (CCTNS), National Intelligence Grid (NATGRID) [that draws upon information available from various agencies that can be made available for the purpose of identifying criminal activity] Centralized Monitoring System (CMS), Unmanned Aerial Vehicles, Close Circuit Television, etc.

Moving on to the question as to whether surveillance is justified and the possible balance to be achieved, Mr. Thakaran said that surveillance is justified in the light of its impact on national and economic security. The security of cyber space cannot be an optional issue but is an imperative need. The best approach to strike a balance between the two is to adopt the principle of Red Flags i.e. pursue surveillance only on some ‘targets’ or ‘suspects’. Technology experts must develop systems which can ensure compliance by the law enforcers. Legislation must ensure personal privacy and governmental accountability in the use of new technology by limiting the collection and use of personal information wherever possible and by imposing disclosure norms. Mr Tharakan, in response to the queries, acceded to the fact that easy surveillance makes us less secure. According to him surveillance is not about politics. The targets are potential criminals who can do harm to the country. He even agreed that current technology doesn’t adhere to existing sanctions and the biggest threat to cyber security comes from Digital Arms Trade.

**Saikat Datta:** Mr Datta said that he was addressing the session in 3 roles: as a journalist, as one under surveillance and as a citizen providing empirical analysis. He took a different stand on the Gujarat issues saying that none of the requests were illegal when seen from the perspective of existing legal procedures and that it speaks volumes about how weak our legal structure is when it comes to monitoring and surveillance. He said that we have moved from an era of fundamental rights to fundamental restrictions. The national strategies constantly tell you what you can't do. He advised us to not take a piece-meal approach towards understanding the issue. There is apparently an assumption that one under surveillance is immediately guilty until proved, meaning that there is a reverse burden of proof. However there is no legal regime as such because of which the solution appears in the form of technology as the only protection against surveillance. In India, it is the bureaucrats' decision. The situation is contrary to England where the courts are approached to handle issues like wire-tapping. Setting up agencies will at least set up a structure and a much desired procedure. In reply to a question, he said that there is a need to codify the regulations and have a strict interpretation of that. Auditors and external oversight institutions will help us keep it in check. The balance is very clear according to him. Individuals have liberty. They always have liberty and there should be minimal reasons to strip them of their liberty.

**Maria Xynou:** Analyzing the Draft national cyber security policy, Ms. Xynou said that it tries to anticipate attacks because of which they have to engage in preventive surveillance. That can be a problematic aspect. Also, another major concern is the sharing of information with third parties as there is no control after it is shared.

She mainly addressed the controversial provisions of the IT (Amendment) Act 2008 that, in her opinion, are Section 44, Section 66A [which contains definition of offensive messages], Section 69 [Interception of any information which mandates disclosure of encryption keys, non-compliance of which shall result in jail sentence], Section 80 [seizure of suspects in public places without a warrant which mostly happens in cyber cafes]. These provisions amount to major human rights violations. These watchers are aided by the Surveillance industry in India. The kind of technology sold, the high biometric surveillance due to Unique Identification (UID) and integration of surveillance technology in day to day life (coca-cola tin can cameras) illustrate the aid and extent of Surveillance Industry in India.

**Jacob Appelbaum :** Addressing the question as to whether surveillance makes us more insensitive, Mr. Appelbaum said that it becomes really hard for people to understand when they don't understand technology. He said that they shall never put a backdoor into Tor because if government acquires one, it will use the same to spy on other governments. A major part of the problem is that we shift the risk from the criminals to civilians by way of surveillance. He said that surveillance should be seen as a tool to control and that everyone's privacy should be respected without making anyone a criminal. He said that it is politics, i.e. politics of effective investigative journalism and there has to be an effective democratic oversight to ensure repression. He asserted that surveillance is political if criminality is political. Law is a tool of masters over slaves. Technology cannot respect the law. The law is abstract. In addition to the threat of arms trade, another haunting threat is the reverse burden of proof. He said that we are innocent by default and when people commit the crime of unjustified surveillance use, they must be convicted. Making evidence obtained through illegal surveillance techniques inadmissible in evidence is pointless. Freedom from suspicion is the greatest asset. One cannot possibly feel free in a world where we know that everything we do is recorded and analyzed based on facts. The technology and machines which have no sense of human justice are becoming our masters. When asked about his conception of the Internet in the question session, Jacob replied that it is the greatest surveillance equipment ever developed. He pointed as to how internet and technology have been increasingly taking command over us. They have become a means to enslave us without even our knowing that we are being enslaved and this is the point where democracy dies- where everyone knows what everyone thinks and how to influence them.

Hence the gist of the session can be covered in three main assertions which formed the core of the discussion on the issue of security and surveillance:

- Mass surveillance does not work. It is not desirable. It is not effective.
- Accountability of intelligence agencies through legislation.
- Laws are outdated and unconstitutional

## DAY 2-MAY 26, 2013: DATA PROTECTION

### SESSION 1: CURRENT FRAMEWORKS FOR DATA PROTECTION IN INDIA: ARE THEY ADEQUATE?

*Data protection mainly ensures that your personal data is protected from abuse by the government, businesses or organisations. There are vast number of avenues on the internet which require the users to enter their personal/professional information. This creates a lot of potential for abuse in terms of the end-use of this data. Thus, a significant theme attached to this topic is that of privacy and one sees constant interaction between the two concepts. Another issue is the duration for which data remains on the server and the appropriate time* *and manner of its destruction. In this session, the panellists discussed the frameworks currently existing in India for data protection, examining their adequacy.*

*The speakers included Col. Mathew Thomas, Mr. Bhairav Acharya, Mr. Rahul Cherian, Mr. Raghunath Ananthpur, and Mr. Samuel Mani. The session was moderated by Mr. Bhairav Acharya*

**Keynote address:**

The day began with the keynote by Col. Mathew Thomas. He set the tone by raising the question of how data protection and cyber security are different. He explained that cyber security deals with the safety of assets (physical or tangible) by preventing their damage or theft on the internet. On the other hand, data protection deals with protection of data of cyber assets as well as of individual data. He further raised a question: Shouldlaws should be used for protecting people,data or both? He went on to highlight as to how by protecting data, we are necessarily protecting people. Another important point raised by him was regarding how the discussion of data protection is generally limited to the middle class and how there is a need to expand this discussion of protection of data to all classes.

He then went on to the highlight the various problems like cyber threats, terrorism and the various legal remedies available for the same. It was seen that the main problem is not lack of black-letter laws to deal with these problems but rather their enforcement. There is no use in seeking new laws when the administration of the existing laws is inefficient. An insightful suggestion made by him was to use technology to overcome such problems. Law can be a very useful tool in overcoming the shortcomings of justice system. An example he mentioned was how the calling system in courts could be replaced with a new technology.

He set the tone for the start of the first session with questions of the reason behind *Aadhar* being introduced as a brand name and identity card when it's just a number.

The first session was on *Current Frameworks for Data Protection in India: Are they Adequate?*

The session was moderated by **Bhairav Acharya**. He laid down the agenda of the session in terms of looking at the current data protection framework. India for long hasn't had to deal with data protection legislation. He discussed how pre-independent India had an interesting principle of privacy and state collection of data. It was said that it was only after independence that privacy as a legal concept and data protection became important. Till 1990's state collected private data. It was accepted that modern nation-state needs data for governing. This situation became problematic when data was collected by private parties and not by the state. He set the stage for the successive speakers by raising the issue of which law should regulate data collection and how. He raised certain issues for the panel such as importance of Section 43A under the Information Technology Act, 2000 and the A.P Shah Report on Principles for future data protection(published in 2012). He put this discussion in perspective by highlighting how misuse of data was harmful and hence, under the harm principle, it was the duty of every state to protect their citizens from the same.

**Mr. Rahul Cherian** The first speaker was Rahul Cherian. He talked about how data protection is a recent development in India. He highlighted that the Indian constitution does guarantee privacy well within the right to life. Unfortunately, data protection did not have strong backing of law until recently. Before the recent legislations, data protection was only secured by contract. AP Shah Committee came up with recommendations on data protection. It highlighted how we need a privacy act based on the constitutional principles to address issues with regard to personal information in this country.

He highlighted some of the important recommendations made by the Committee. This included issues of inefficiency in government system and the need for a regulator dedicated to privacy and data protection. The report also laid down that limitations with regard to right to privacy were only admissible to the extent that freedom of speech was limited. One of its major recommendations was to harmonise various privacy laws across industries. The Committee also said that there is a need for self-regulating aspects based on national principles.

It laid down principles that there should be notice given whenever data is collected in terms of what, how, for what and how it will be disclosed. It also said that data can't be collected for all encompassing purposes. Disclosure of information also limited. Its main aim was to bring home the point that the overarching principle of privacy can't be subsumed for commercial interest. Mr. Cherian then focussed his attention to the IT Act, 2000-the first act in India for protecting data. Though this act had provision with regard to confidentiality obligations but it was only imposed on government agencies. The 2008 amendment to the act came in the form of Section 43A and brought a stringent regime with regard to data protection. It laid down that data protection can be secured by contract or even in its absence, under principles of the act. He then talked about the IT Reasonable Practices and Procedure Rules, 2011 and the Press Release by the Ministry. He highlighted the confusion created by latter as to the scope of its application.

He went on to describe how contracts may not always work for data protection with regard to individual rights. If individuals adopt the measure of contract, they don't have to comply with the principles under the act. Other industry-specific data protection regimes available were also discussed by him. He highlighted how RBI has a regime which makes it clear that disclosure must be by consent and for only the purpose stated. Insurance and banks don't allow cross selling unless express consent taken. Credit info also can't be disclosed. He concluded by highlighting the need to harmonise all the existing legislation providing data protection with a national level, overarching law.

**Mr. Ragunath Ananthpur**: Ananthpur began his speech by putting forward his agenda. He emphasised that he would be discussing the background of rules the key concepts stated therein such as sensitive data, disclosure conditions etc. Further, his agenda was to compare these provisions with the UK Protection Act, 1998.

He began by highlighting how the debate for data protection became important once India became prominent in the outsourcing business. Lack of data protection would have led to loss of outsourcing business. He also brought attention to the fact that the European Commission doesn't include India in the list of countries providing adequate level of data protection.

He laid down how data protection rights are categorised into personal information and sensitive data and under the rules, protection is only given to sensitive data. Sensitive data includes passwords, bank account, sexual orientation etc. while personal information is related to the natural person. The standard is higher for protection of sensitive data than personal data. The data protection rights apply to body corporates excluding government agencies. While summing up, he said that the Privacy Act should consider the basic principles followed by the European Union and other large data-exporting nations so that Indian nations are not prejudicially burdened.

**Mr. Samuel Mani**: Mr. Mani began by looking at the theoretical framework of where we are today and where we need to head in the context of data protection and privacy. He conceptualised privacy as right to be free from unauthorised intrusion and having control on how one's information is used. He then discussed how OECD laid down principles for data protection which formed basis for the EU discussion as well. The eight principles are collection, limitation, quality of data, purpose specification, limit the use to purpose, secure the data, openness, individual participation and accountability.

He highlighted these issues in terms of their applicability in mobile telephonic industry by talking about how mobile companies use data for advertisement campaigns. Though this doesn't seem to be a problem on the outset, it becomes a problem when the company shares this data with third parties. The mobile companies make disclosures to the government if it seems problematic to them. He described the micro-tracking process of Google, which track the activities visitors engage in before making purchases, such as creating an account to make its advertisement campaigns as an illustration of the larger issue.

The issue according to him wasn't that these practices exist but that there are no rules to deal with them. The fact that you have no control over these activities is a major disabling factor. The practices would inevitably result in unwanted intrusions. This is what raises a need for a law to deal with this: determining the way one's data is collected and used. One needs to be made a willing participant in this process. The individual should have control over the use of his data. It is also not that companies can't do business in a regulated system; it's just that it hasn't been done in India due to other priorities.

He predicted that after consumer rights, privacy would be the next big battle ground between the businesses and the individuals. He believed that it's better for the businesses to adopt regulation so that they don't have to re-engineer later.

The session came end with discussions among the panellists and the audience on the issues raised by the speakers.

## SESSION 2: COMPARATIVE ANALYSIS OF DATA PROTECTION FRAMEWORKS: WHERE DOES INDIA STAND?

*A data protection framework controls the giving and end use of data provided by users. Accordingly, many nations have formulated such frameworks, especially in the light of larger amount of confidential and personal information traded on the internet. In this session, the panellists discussed the various data protection frameworks to locate India's position in the same. The discussion would also help examine the veracity of the European Unions claim that India lacks adequate data protection The framework, if found inadequate, would raise* *concerns not only for civilians but also for large-scale businesses that function on outsourcing by developed nations.*

*The speakers included Ms. Nadezhda Purtova, Ms. Rakhi Jindal, Mr. Prashant Iyengar, Mr. Aradhya and Mr. Sarthak.Gupta .*

**Ms. Nadezhda Purtova**: Mr. Purtova introduced the discussion on comparative analysis of data protection frameworks. She spoke about the EU Data Protection Directive 95/46/EC and stated that personal data could be processed, *inter alia*, with unambiguous consent of the data subject. This had roots in privacy and protected the rights of self-determination. She also stated that the Draft Regulation of 2012 (which seeks to supersede the EU Directive 95/46/EC[26]) moved away from self-determination and it had no reference to privacy.

**Ms. Rakhi Jindal**,: Ms. Jindal proposed to lay out the comparison between the India and the European Union with regard to the data protection frameworks. She first stated that there was no data protection regime in India for the longest time.. The Constitution of India and the law of torts were the applicable law, but they were insufficient as the provisions of the former were enforceable only against the state and the effectiveness of the latter was uncertain. Even currently, the Personal Data Protection Bill has not been passed and the stop gap solution lies under the Information Technology Act which deals with data protection. Under the European Union (EU) law, there were a lot of directives dealing with data protection. A second key difference is that in India, the types of data which are protected are personal data, which could identify an individual, and sensitive personal data, which iscapable of identifying a person based on, *inter alia*, her password, financial information, sexual orientation and medical records. The sensitive personal data is protected only when it is in the electronic format but by interpretation, personal data is protected even when it is not in the electronic format. Under the EU law, there are compliances for personal data as well, which is different from the position in India. Another point of difference in this regard is that in India, there is no protection of information about political opinion, and further, only digital data gets protection.

She moved on to discuss the second aspect of the comparison between these jurisdictions, namely that of consent. In India, there is no consent required for the collection of personal

[26] http://www.mlawgroup.de/news/publications/detail.php?we_objectID=227

data but for sensitive personal data, written consent is required. This also includes electronic consent. She gave an example of electronic consent-that of the ‘I accept’ which users tend to click on. Further, there is a specific opt out provision with regard to the sensitive personal data, (wherein if the provider opts out of providing consent, the company could decline to provide either the goods or the services for which the information was sought[27]). She felt that this could create a possible grey area as under instances wherein an employer who wished to collect the sensitive personal data of the employees and the employee opted out of it, the issue of which ‘services’ are provided by the employer arises. Under the EU law, the data subject had to provide consent for all kinds of data. Further, for the special categories of data, it cannot be processed unless the data subject makes the consent public, which is subject to confidentiality restrictions, and the data subject could object to the processing of data on ‘compelling legitimate grounds’ or where it was used for direct marketing. In light of this, she also made a reference to the position under Indian law where there are no grounds for objecting to spam e-mails.

She then spoke about the third aspect of this comparison, that of registration requirements. Under Indian law, no registration is required for personal data but registration is required for sensitive personal data. Under EU law, it is more sophisticated as states have to establish a national authority. As under Indian law, no compliance was needed for personal data, as opposed to sensitive personal data but for both these categories of data, reasonable security practices and processes had to be maintained. Under EU law, the measures have to be appropriate with regard to the nature of data being processed, and resources and finances available to the data controller need to be looked at.

In the concluding part of her speech, she threw light on the aspect of enforcement. Under Indian law, only the data subject could initiate proceedings for civil remedies, and the police inspector could initiate proceedings for criminal remedies whereas under the EU law, the states had to enact provisions.

**Mr. Prashant Iyengar:** Mr. Iyengar started his speech by talking about the older legislations in India such as the Evidence Act and the Transfer of Property Act, and stated that just like these laws, privacy law and data protection seemed to ‘echo’ the laws in the West. The laws on privacy and data protection were carelessly worded. He added that the data protection law ‘resided in the EU’.

[27] http://www.dlapiper.com/india-issues-game-changing-data-privacy-regulations/

He then spoke about the aspect of adequacy and stated that for determining the aspect of adequacy, the surrounding circumstances of a data protection operation would be evaluated.

He also said that the EU had some concerns about Indian laws. First, under an agreement between parties, there was an issue whether they could disregard s. 43 of the Information Technology Amendment Act. He felt that s. 43 would apply, but that there was room for interpretation. Second, for reference between parties, it was unclear whether it included only consumers or whether it included contracting parties as well. He felt that two arguments were possible as under s. 43, the term 'person affected' had a very wide ambit hence it would include consumers but the terms 'wrongful loss' and 'wrongful gain' under s.43 could be understood narrowly so as to not include consumers. Third, in light of the purpose-limitation, namely, that data collected should be only used for the purpose it is collected for, the only law which applied to this was the 'reasonable security practices and procedures' [under s 43(ii)] which meant that the purpose limitation applied only to sensitive personal information and not to other information and hence it could be said that data security applied only to sensitive personal information.

**Mr. Aradhya and Mr. Sarthak (Student Speakers)**:

Mr. Aradhya and Mr. Sarthak spoke about the debate on the adequacy assessment requirement. Mr. Aradhya stated that it had three problems. Firstly, it interfered with the domestic standard of privacy. Secondly, it excluded domestic priorities. In India, the focus was on increasing access to the internet and hence more advertisements could be useful for greater use. Thus, the priority in India may not be data protection. There was a difficulty in accommodating the adequacy requirement because when data was coming in from various places, there was a want for accommodating these different requirements of adequacy. He proposed an alternative framework wherein there had to be a shift from data security.

Mr. Sarthak elaborated on this alternative framework, and stated that there had to be a new model based on the existing alternatives. He felt that adopting Binding Corporate Rules (BCR), which are internal rules adopted by multinational groups of companies that define their policy with regard to transferring personal data was time consuming and expensive, but the Safe Harbour Agreements(SHA) had benefits. These are streamlined processes that allow local companies to comply with EU standards for the protection of personal data. Hence they proposed that EU and India sign an agreement similar to the SHA singed between the US and the EU.

## SESSION 3: FUTURE FRAMEWORKS FOR DATA PROTECTION IN INDIA: HOW DO THEY DEFINE PRIVACY FOR INDIA?

*The concept of data protection is closely integrated with that of privacy. A particular use of user data can potentially infringe his/her right to privacy unless done with consent. Thus, to what extent has the user waived right to privacy when feeding information on the internet is of the essence. This is dependent on factors such as the platform on which the information is provided, the query in response to which the information is given and the amount of information which can be said to fall within 'public domain'. Whether public domain has same implications for print and electronic media is also debatable.*

*The speakers included Mr. Bhairav Acharya, Mr. Apar Gupta, Ms. Shreyashi Sengupta and Ms. Roopashi Khatri.*

**Mr. Bhairav Acharya**: Mr. Acharya introduced the discussion on future frameworks for data protection in India. He gave a broad overview of the Draft Privacy Protection Bill.

He stated that the Bill omitted spam completely from its framework. He also gave an overview of the constitutional framework, as under the Seventh Schedule of the Constitution of India, the Parliament could legislate upon matters based on Information Technology, based on the residual entry, Entry 97. However but police powers were under the State List and criminal proceedings were under the Concurrent List, and hence before deciding on Committees in this regard, the Centre's competence needed to be looked at.

He outlined certain points regarding how the future law should be like. He stated that people should have a right to privacy, and it should not only be restricted to citizens. A future law should also incorporate the OECD principles and the principles of the Justice A.P. Shah Committee Report, and there should be an independent watchdog instead of a Commission, to determine its staff and to vote on its own finances. He also looked at the issue of the Bill ousting the civil jurisdiction of the lower courts and vesting it with the independent commission, and questioned how the two-appeal process could be maintained.

**Mr. Apar Gupta**: Mr. Gupta provided a historical background of privacy. He stated that the earliest examples of privacy rights were with respect to easements, where one person's window opened into another and hence due to this, the Indian Easements Act was enacted.

He stated that the case which was most relevant now with regard to interception and surveillance and the issues raised by this panel was PUCL v. Union of India (1997). It was held that there were certain grounds for interception (It was held that Occurrence of any public emergency" or "in the interest of public safety" are the sine qua non for the application of the provisions of Section 5(2) of the Act[28]).

He added that there was a difference between the letter of the law and practice regarding how these safeguards were imposed and enforced, which was reflected in the Nira Radia and the Amar Singh case. He also stated that in context of the general issue of privacy, surveillance had to be taken into account or else it would be a half-hearted measure.

**Ms. Shreyashi Sengupta:** Ms. Sengupta spoke about the industry view on the practical challenges regarding privacy. She illustrated this by giving the example of a case wherein when a person made a phone call, the employer listened, when he sent emails, the employer checked to make sure he wasn't compromising on the company's information, and hence the employer could basically do what he wanted. She also illustrated privacy concerns in banks, and stated that banks were the custodians of a lot of private information, and that 47% of the banks in India understood what privacy was, and 87% understood that privacy issues would grow in scale.

She, however, felt that India is far behind as compared to other countries as privacy is not in the Indian culture. It was treated as a regulatory compliance rather than an operational compliance. She said that privacy was not just an issue relating to Information Technology, and that she would like to see the privacy culture in every department, and having a law would help in that regard.

**Ms. Roopashi Khatri (Student Speaker):**

Ms. Khatri, a student at NLSIU, spoke about the Justice A.P. Shah Committee Report on privacy. She provided a backdrop to privacy by discussing the landmark Kharak Singh[29] case wherein the court observed the importance of security of one's privacy against arbitrary intrusion. She then made a reference to the nine principles of privacy under the report.

[28] Telegraph Act of 1888.
[29] Kharak Singh v. State of Uttar Pradesh, (1964) SCR (1) 332.

She stated that the report had simplified privacy law, as there was an idea of reductionism as privacy had been reduced to nine principles, which did not capture all the aspects of privacy. The report missed out on the control of a person's information and the principles did not deal with how the data subject was supposed to control his information. She felt that the control of the individual should be emphasized.

## SESSION 4: GOVERNANCE SCHEMES DATA PROTECTION AND SECURITY – WHAT IS MISSING?

*This session is closely linked in topic with the previous one, and focuses on the existing schemes of the government which require the use of data protection and similar security procedures. The main scheme in consideration is the Unique Identification or 'Aadhar' scheme and the panelists have discussed the concerns attached to its collection and storage of data, more significantly in the light of the public-private partnerships acting in its stead.*

*The speakers for this session were Col. Mathew Thomas, Mr Somasekhar VK and Mr Aditya Sondhi.*

**Col. Mathew Thomas** began the session by highlighting his experiences in Soviet in the early 1970s, which was a 'surveillance society' as well, creating fear in the eyes of the people and having the State regularly impinge upon the lives of its people.

The advancement in technology and the increase in surveillance have equated Dictatorial Russia with the Western World. The actions in the Gulag Archipelago cannot be distinguished from what is happening in Guantanamo Bay, although it is called by the name of "democracy". The "Technological Tsunami", which began with the first IBM computer, is brushing aside every sane voice of caution. Technology is necessary but there are limits to where it can and cannot be used. What is problematic is that current technological solutions go around looking for problems to solve.

He further argued that there is an identification epidemic currently in place. They are under the extraordinarily popular delusion that if people can be identified, they can be controlled. It is to be kept in mind that identities can be stolen and misappropriated. He proposes the use of sampling instead of collection of data through the census as being far superior, easier and cheaper. This can be conducted by a number of companies while deciding the markets for their products. Moreover, it has been recognized that collection of 100% data brings in at least 15% defectives. Data is collected at enormous costs and is also prone to misuse.

Col. Thomas proceeded to explain the overemphasis placed on data collection in government schemes, as highlighted with the UID example. Data collection is based on the false assumption that a lack of identity prevents the poor from collecting benefits from government schemes. The government claims that welfare subsidies are siphoned off and the UID will prevent this, but this is untrue. This can be shown with the example of the PDS and the LPG system. India has around 6 lakh PDS shops – Karnataka alone has 4000 of these. The government cannot spend money identifying these shops in the first place and then equipping them with proper electronic mechanisms to read UID. The change from provision of food to conditional cash transfers is also not workable. While the latter scheme was successful in Brazil in making children go to school, it would not work in case of PDS. Furthermore, the real problem in the PDS system lies in storage of grains. Almost Rs. 80,000 crore worth of grains are lost in storage. There is a need to focus on this instead of data collection.

RTI queries conducted by Col. Thomas reveal that, according to the department of civil supplies, no fake ration card was detected in Karnataka with the help of UID. On the other hand, the UIDAI stated that its mandate is to only issue UID and not check and detect fake ration cards. This presents an inherent contradiction as UID is openly claimed to be used to eliminate fraud in the PDS system.

Similarly in case of LPGs, it is said that no document/working paper is available to show how cash transfers will be done. The problems with the system can be highlighted with the help of an example. The connection for LPG may be in the name of one person. But this does not account for situations where the ID holder is not home or if their staff or relatives are to make the collection on their behalf. Is it possible then to connect their UID numbers? He added that the existing consumer number database is sufficient for these purposes and there is no need for a separate UID.

The collection of Biometrics also presents problems as it cannot be captured in many cases – for example, the biometrics for senior citizens above 75 years of age are not clear. Further, there is no information on how this data will be used.

The government has undertaken the ‘deceit of voluntariness’ and has used a package of threats and inducements to make people enroll for UID. Its departments regularly ask for the same, making it mandatory. For example, in Chandigarh, the RTO requires the UID number for a driving license.

He highlighted some of the dangers to security posed by the use of UID:

1) Process and authorities collecting data– One of the companies which acted as the enrolling agency for UID has been accused of fraud in a civil supplies contract. The people believe that they are providing data to the government while it is being given to a contract employee who is selected without due diligence by the government. In a number of places such as Pune and Mumbai, private people set up enrolling shops and the government has made no effort to prevent this.
2) The casual attitude of the government – Half a million peoples' data has already been lost. The government tried to make excuses that data is not lost but could not be decrypted, but there is no conclusive information on the matter.
3) Persons having control of the data – There is a possibility of use and abuse of data. The UIDAI is not accountable to parliament. Its Chairman has powers of a cabinet minister. The UID is not backed by any law or notification. It is directionless, non-transparent and a threat to national security.
4) Inability to appreciate that all data is sensitive – All data from names to places of residence is sensitive; for example, names point to religion of the person and place of residence gives an indication of their economic position. By linking information in such a manner an enormous amount of data can be obtained.

Further, concerns of privacy increase according to him as people become increasingly 'transparent' whereas the government remains as opaque as always.

The UID is fraught with problems. Agencies have been caught selling data and the government has no measure in place to protect these people. Further, computer systems fail to pick up errors in many situations, such as if someone's biometrics is compromised, it is not possible to get it redone. The UID thus creates a new identity for you which is based on how it is defined in the database rather than reality. Colonel Mathew concludes by taking an extreme stand on the issue, suggesting that no law can apply to this situation and regulate the usage of data by the UID and as a result the project ought to be scrapped for its excessive reach and intrusion into privacy as well as its inability to protect sensitive data.

**Mr. Somasekhar-** Mr Somasekhar began his address by defining the consumer and the eight rights specific to them, of which two are missing in the Indian context, namely, the right to basic needs, and the right to health and environment. According to him, India has the best Consumer Protection Act in world but the problem lies in implementation. People need to take control of their situation and not give data blindly. As a result, the demand for consumer privacy should become a ninth right of consumer.

New ideas for data collection are invading personal lives and trying to figure out the pattern of purchase of consumers, thus threatening their privacy. As a result, the government should prioritise the enactment of a data protection regime and its enforcement. It is not the collection of data which is problematic but its utilisation. The processes have no due diligence standards, and there have been instances where the enrolling agencies have not transferred data but the government has conducted no enquiry. Data is not destroyed once collected but kept aside and this can be misused by anyone.

Mr Somasekhar ended his discussion by emphasizing the need for people to demand protection as consumers, rather than voluntarily providing personal data and together standing up for the protection of these rights.

**Mr. Aditya Sondhi** was the last speaker. He sought to make a larger point through the subject of discussing the general lack of regulation/ statutory framework existing in India for dealing with information, privacy and human rights of Indian citizens.

Intelligence agencies are exercising far reaching powers, including powers of surveillance without constitutional or statutory basis to support their purpose. This *ad-hoc ism* is troubling. The rule of law needs to be maintained in the Indian society. Executive orders, government orders and notifications are not enough when authorities created under it have far reaching powers that can violate constitutional rights.

The right of privacy of citizens emboldened by international instruments such as the Universal Declaration on Human Rights (Article 12) and the decisions of the ECHR (litigation relating to surveillance of an individual who was part of the civil liberties movement). This has led to enactment of surveillance legislations in countries such as the United States and Canada and further legitimized many intelligence activities. Such laws are not found in Pakistan or China. Unfortunately, India, too, does not have these laws. There is no law on even information gathering. Surveillance is common place and even the President was subject to the same.

The sort of equipment used, the mechanism and its reach is overwhelming. Mr Sondhi mentioned that he himself was a subject of surveillance when he filed a PIL on the issue. He described how it is a terribly obnoxious feeling to know matters are not private and your

SMSs and calls are being read and listened to. The extent and reach of the state is enormous. UID is just one small aspect of the above.

The RTI Act also contains barriers. No information is to be provided unless it relates to human rights violation. But it is impossible to prove a violation when you are stopped at the threshold and not allowed to access information in the first place. UID has become a status symbol and the masses have come to believe that it is necessary to sign up for it. Further, no law has been passed pertaining to the UID, although a notification was issued in 2009 and a Draft Bill was created. The government has thus been acting ex-post facto, which is unsustainable.

Firms privy to the project are closely connected to US and enjoy extensive protections there, created serious threats to the Indian citizens. Much of the information which is gathered in India is up for sale. These sorts of exercises are given an innocuous colour by state as they are presented in terms of national identity, provision of services. But there is something inherently wrong in collecting information without basic checks and balances. And these cannot be subsequent to the process or done by the judiciary.

Mr. Sondhi further alleged that the government has hoodwinking the people, while civil society has not questioned the misinformation being circulated with regard to UID. He did not present any opinion on whether the UID ought to be continued, but rather concluded by advocating the legitimisation of the process by forming a strong foundation for it in law.