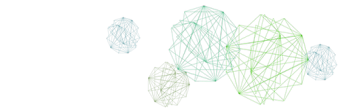

SYMPOSIUM ON HUMAN RIGHTS & THE INTERNET IN INDIA

Organised by

Global Network of Internet and Society Research Centers

UNESCO Chair on Freedom of Communication and Information at the University of Hamburg

Alexander von Humboldt Institute for Internet and Society (HIIG)

Hans Bredow Institute, University of Hamburg

&

Centre for Communication Governance at National Law University, Delhi

REPORT OF PROCEEDINGS

January 17, 2015

Authors: Ujwala Uppaluri & Rahul Gullaiya

TABLE OF CONTENTS

INTRODUCTION

The Centre for Communication Governance (CCG) at National Law University, Delhi (NLUD) in collaboration with the Global Network of Internet and Society Research Centres, the UNESCO Chair on Freedom of Communication and Information at the University of Hamburg, the Alexander von Humboldt Institute for Internet and Society (HIIG) and the Hans Bredow Institute, University of Hamburg, organised a Symposium on Human Rights at 5:00 p.m., on January 17, 2015 at the India International Centre, New Delhi. The Symposium was split into two panels:

1. Surveillance and Databases: Experiences

2. Privacy Concerns and Unpacking the Intermediary Liability Debate in India

WELCOME ADDRESS

Professor (Dr.) Ranbir Singh, Vice Chancellor of the National Law University, Delhi delivered the Welcome Address. He said that it was an honour for the National Law University, Delhi to host the symposium and thanked each of the co-organisers for helping realize it.

He noted that the National Law University, Delhi has been committed to contributing constructively to important debates around the law in India. It encourages and supports a range of research and policy work, through activities such as working with reform efforts with the Law Commission of India. He made special reference to the Centre for Communication Governance, mentioning that it was started by a very energetic group of young scholars. He saw it as the most successful of the National Law University, Delhi efforts so far – despite being only two years old, it has already begun to have tangible impacts on policy in law reform not in India and abroad. He explained that tracking, explaining and improving the processes through which censorship and surveillance take place in India across the media has been a key preoccupation of the Centre for Communication Governance since its inception, given that these processes affect a range of closely held fundamental rights including the freedom of expression.

He said that he was certain that the discussions at the symposium would be very engaging, given the expertise that each of the panellists brought with them. He was certain that the discussions would demonstrate how important these issues are and hoped that they would offer food for thought about how one could begin to address these issues.

He then went on to touch upon the Winter School, and said that he was looking forward to the discussions there around surveillance and data protection law. Concluding his Welcome Address, he thanked the panellists for generously agreeing to conduct some of those sessions, welcomed all the students who were present and extended his warmest greetings on a cold Delhi evening to the gathering.

INTRODUCTORY REMARKS

Professor (Dr.) Wolfgang Schulz, Director, Alexander von Humboldt Institute for Internet and Society delivered the Introductory Remarks.

He opened by expressing gratitude on his behalf and on behalf of the German students present for being invited to participate in the Winter School that would follow the Symposium.

He then talked about the Network of Centres. He said that it was extremely interesting to be a part of this family of centres of internet research working on an international scale. The Network was started about three years with a big conference with their friends and colleagues attending at the Berkman Center at Harvard University, where the idea to form a network with all those involved with research in internet and society issues from different disciplinary perspectives was born. He noted that some centres were extremely active in this network, and that the Centre for Communication Governance here in Delhi was among them. He said that the idea behind the Network was to create a structure to support all the institutes and their efforts to do research on internet and society issues, and to create synergies to help them to work together, and engage in comparative work. The first years of the Network were spent in conferences learning what each of the member centres were doing and understanding their backgrounds. Efforts have now moved forward and the Network has some ongoing research projects. One research project around internet governance had just been published. Prof Schulz also mentioned that ICANN, a very important player in the internet world, together with Foundations provided seed funding to the Berkman Center and the Network of Centres to come up with ideas about internet governance. He said that the first package of case studies about internet governance issues had been drafted and that the second big project was closely related to the issues about the governance structure of online intermediaries. He reported that the Network had been successful in curating different case studies on the subject, noted that the situation in India was extremely interesting and emphasized that these efforts had demonstrated how important it was to do comparative analyses of the consequences of different styles of regulating.

Concluding his remarks, Prof Schulz said again that he was very happy and proud to be a part of such crowd and hoped that in that late afternoon all would together discover some interesting

things and have some insight so that everyone left the room with some enlightenment at least as regards internet governance and data protection.

PANEL I: SURVEILLANCE & DATABASES

Panel Discussion

Professor K.S. Park, Former Commissioner, Korea Communications Standards Commission and Professor, Korea University Law School opened the discussion on Panel - I.

Prof Park's talk focused on the South Korean experience with state held databases, and the Resident Registration Number (RRN) in particular. Every Korean born in Korea is given an RRN automatically, and it is nearly impossible to change throughout that person's life. It was invented in the 1970's for the purpose of identifying spies from North Korea and was given to people born in Korea after the division – so, if someone could not produce his RRN then the assumption was that he must be from North Korea.

As Government worked to make the identification system foolproof, the perception that the RRN was reliable began to spread, so that more and more public agencies that had nothing to do with national defence or catching spies began to use RRNs as the preferred identification. Social services, for example, started requiring an RRN. Private sector operations, such as banks also began to require RRNs. Even the purchase of mobile phones now requires the production of an RRN, not by law, but because telecommunications providers see it as reliable. As a result, today, many companies and agencies hold large databases of RRNs.

Prof Park problematised this state of affairs, pointing out that as the number of databases holding RRNs proliferates, the number of companies and agencies relying on RRNs as identification increases, as do the number of surrogates, or substitutes. This means those attempting identity theft now had whole treasure boxes of data that they could target.

Prof Park termed this the 'paradox of trust' – when Governments try to create a trustworthy identification system, private and public sector agencies use the system and store the identifying information in their databases. This offers hackers far more targets than before for identity theft. The consequence of these increased thefts would in turn reduce trust in the system.

He then noted that function creep, the tendency of using an identification system for purposes other than its originally intended purpose, was a significant concern. Prof Park pointed out that

this tendency would also have the effect of reducing trust in RRNs as a whole. He pointed out that many countries that had identification systems also had laws that limited the purposes for which their contents could be collected. This has, however, meant that for different purposes, one person would carry many different identification numbers and there would not be one number that could represent a person across the many areas of his life.

Prof Park then discussed the state of the law. South Korea has a provision in its Personal Data Protection Act that bans any collection of data unless it is expressly allowed or required. In other words, unless the Legislature or the Government specifically permits or requires collection of the RRN, it cannot be collected. Prof Park opined that this law had not been effective – at his last count, there were eight hundred and sixty six such laws and regulations which permit collection of the RRN. Koreans must disclose an RRN even to issue a book at a library.

In 2007, a law which required that persons posting content online had to first register a name and RRN with the internet company was enacted in South Korea. Prof Park argued that this law interfered with free speech and did not serve its intended purpose. In his opinion, there was a greater chance of the paradox of trust arising online. He counted six or seven studies which showed that there was no decrease in illegal information being posted online after this real name requirement was put in place. In 2012, the Constitutional Court in South Korea found this requirement unconstitutional as it amounted to prior censorship.

Dr. Usha Ramanathan, Independent Law Researcher was the second panellist on Panel - I.

She opened by addressing the question of why privacy is a problem in India. In her view, the general perception in India is that privacy is not a critical issue to Indians, and that there was little debate around the fact that the Government will invade privacy in return for the provision of services. She said that since surveillance actity was not yet seen as an issue primarily about privacy, there is little public outrage about the state's activities despite its extensive infringements of citizens' privacy. She also pointed out that the Indian media had not focused on these infringements in any detail to create public awareness of the issue.

Dr. Ramanathan then listed some databases that exist in India with the support of the Government, and which invade privacy: the National Population Register, the Unique

Identification Number database, the DNA database and the National Intelligence Grid. She also noted that the Collection of Statistics Act, 2008, and the levy of the Goods and Services Tax also involved privacy invasions. She pointed out that not all of the databases she had mentioned were strictly government databases – they were created with the assistance of the Government but are not held by it. Illustratively, she pointed out that the Unique Identification project went so far as to empower wholly private persons to go to the homes of citizens and lawfully demand biometrics, such as their fingerprints, iris scan, and so on.

She then pointed out that there is neither a privacy law nor a data protection law in India. She also expressed her disappointment about the fact that when a bill on protection of data that was collected and that was to be collected under the Unique Identification scheme was introduced in Parliament, it was rejected.

In the context of the conduct of databasing and related activities by the state, Dr. Ramanathan highlighted the importance of the State being transparent. She noted in this context that the Right to Information Act, 2005 had been a very significant step towards enforcing transparency.

She thereafter went on to describe three ways in which the Indian State is infringing individuals' privacy. She first mentioned the use of the fear of penalties against citizens who refused to give information or who gave wrong information. The second was the promise of welfare in exchange for citizens making themselves visible to the State by enrolling into the database. The third was data collection in the garb of disbursing subsidies – because the subsidy given to the citizens can be tracked, the citizens themselves can also be tracked.

In the context of the National Population Register, Dr.Ramanathan also explained that there were orgaanized efforts to bolster enrolment. She gave the example of an advertisement being run before the start of the movie in Chennai's cinema halls. The advertisement is an appeal to enrol in the National Population Register. She described the advertisement with some levity: one person throws mud which lands on a second's face. He also throws mud and it falls on a third person's face and so on. In the background, these words are sung:

"*Tere desh ki mitti tujhe pukare, Bharat ka vasi hai tu, vasi garv se batla re, O jud ja re…*" ["The mud of your country calls you, You are a resident of India, Oh resident, say this with pride, Oh come and join….."].

Towards the end a voiceover says:

"*Mittise hi shaan, Mitti se hi pehchaan, Baniye hissa National Population Register ka, Camps shuru ho chuke hain, Rashtriya Jansankhya Register, Meri Pehchaan, Mera abhimaan, Bharat Sarkar dwara janhit mein jaari*." ["Honour from mud, Identity from mud, Become a part of the National Population Register, Camps have started, National Population Register, My identity, My pride, Issued in public interest by the Indian Government."].

She pointed out that the National Population Register has not been well-received even among corporate India.

Dr. Ramanathan then argued that each time a biometric is taken by the State under the Unique Identification Scheme, the State acts illegally. She opined that the State acts in this regard as if it is not bound by the law. She noted that the Chairman of the Unique Identification Authority of India (UIDAI) once argued that the citizens of India would have to barter their right to privacy in return for the conveniences that a Unique Identification Number would open up access to. She further said that the State was inducing people to enroll under the Unique Identification Number scheme by providing , for example, a bank account on enrolment. She argued that there was no connection whatsoever between the problems that the UID scheme purports to address and the solutions it provides.

By way of juxtaposition, she requested Prof Park to describe how the Korean state uses biometrics. *Prof Park* replied by saying that in Korea, by the age of eighteen, it is mandatory for every Korean to submit their fingerprints. These, however, are only used by the police.

Dr. Ramanathan then returned to the subject of the UID scheme, informing the room that the slogan of the Unique Identification Number project is the three U's: Unique, Ubiquitous and Universal. 'Unique' means exclusive. 'Ubiquitous' means something which is present everywhere. 'Universal' means applicable to everyone. If these meanings are applied to the slogan of the Unique Identification Number project, she explained that it would mean that the

UID creates a record of personal information for each citizen which will be exclusive to him or her, which will be present or appear across all the state's databases, as part of a system which will be applicable to all Indian citizens.

She pointed that this was not achievable. Even if fingerprints and iris scans are registered, she described how these could change over time (through manual labour, in the case of fingerprints, for example). As a result, a citizen who had registered earlier might not match the fingerprints and the iris scan recorded against his or her name in the database. She pointed out that this would mean that the particular citizen would lose his identity since, in the eyes of the State, he would no longer be the same person. She referred to a 2006 report by Wipro, a large indian company, which indicated that if the State were to continue act as it is acting, the Unique Identification Number would become absolutely mandatory and no one would be able to function or move freely in India without a Unique Identification Number. Despite this, she noted that there has been very little public debate about the UID Scheme.

She also pointed out that the system of recording biometrics in India was started without any testing whatsoever. Given that biometrics may not stay the same over time, they would no longer afford a citizen a unique identification as the scheme intends. Realistically then, the citizen would not have a Unique Identification Number, only his or her biometrics will.

In Dr. Ramanathan's opinion, one reason for this reliance on biometrics is that the Indian biometrics industry, which was previously engaged in military operations alone, is now looking to expand into civilian arenas. She expressed the worry that if this scheme continues in its present form, then the time is soon to come when, without a Unique Identification Number, there would be way to access cooking gas or pensions, and as the project progressed, no registration of marriages, no renting of houses and no purchasing mobile phones without this identification.

Concluding her talk, she noted that a few features of the Indian system have helped to restrain the progress of the Unique Identification Number system. These were circumstances like the anarchy in India, the high density of population and the tendency of systems being born and dying in India.

She ended pointing out that she is not aware of any philosophical thinking or writing about privacy and identity issues in India, and hoping that they could add to the argument against programmes like those underway in India today.

Mr. Saikat Datta, Editor (National Security), Hindustan Times was the third panellist on Panel - I.

He started by discussing the user's perspective of surveillance in India. He opened by sharing an anecdote from personal experience – In Delhi, he had noticed that there was a group of people following him some time ago. This had continued for a day or two, and his friends advised him to approach the police. When this happened again, he asked his journalist friends to be ready to record this with their cameras. He eventually discovered that he had been followed by Government officials, working with the Intelligence Bureau, one of India's intelligence agencies, who were following him because he had written an article on the agency and these officials were curious about how Mr. Datta had sourced and collected his information.

Mr. Datta then expressed surprise about India's transformation from a champion of the international human rights system in the Nehruvian period to a State opposed to providing them under the garb of sovereignty over time.

He proceeded to discuss India's surveillance regulation framework in the context of this opposition of the Indian state to be held accountable for its human rights violations. He observed that the Indian framework was not very different from other regimes internationally – the object was not upholding laws but exercising control. He said that in India, laws born in a colonial framework to surveil still continue in operation. He cited two statutes – the Indian Telegraph Act, 1885, and the Official Secrets Act, 1923. He informed the room that a civil liberties group had challenged the surveillance law in the Supreme Court of India in 1996. He also noted that there had been lack of parliamentary debate before the passage of the more modern legislation, dealing with the Internet, the Information Technology Act, 2000 and the rules framed under it.

Despite the shared history, Mr. Datta went on to explain how surveillance regulation in Great Britain differed greatly from the Indian system. In Great Britain, to put a check on the increasing cases of abuse of surveillance laws, the Security Service Act, 1989 and the Intelligence Service

Act, 1994 were enacted. No similar mechanism exists in India. We have two agencies empowered to undertake surveillance. One, internally, is the Intelligence Bureau (IB), and the other is the external intelligence agency, called the Research and Analysis Wing (RAW). Through a Right to Information application, he explained that he had found that the Union Home Secretary to the Government of India (who is empowered to sanction surveillance applications) had cleared 300 such applications just in a day's time.

He then noted that the National Intelligence Grid (NATGRID) is empowered to tap into twenty two databases proactively to monitor behaviour for investigative agencies and undertake predictive analysis based on this information. Mr. Datta saw the predictive analysis model as a deeply flawed approach, as it would have the tendency to overinclude - when the State applied this type of analysis, everybody becomes a suspect – anyone doing something which he or she does not do on a day-to-day basis enters the State's data system and will always remain in it as a suspect in the eyes of the State.

Mr. Datta then threw light upon the Central Monitoring System (CMS). He said that the Indian Government was very worried about leaks of intercepted data, and had brought in the CMS to prevent this by removing middlemen such as internet service providers. As a result, only the Government would know whose information is being collected and what its contents are. He explained that the State had, in effect, created an entirely opaque system in which the small chance the citizens previously had in occasionally discovering illegalities through leaks had been nullified.

He then went on to explain that the Indian State's approach to surveillance over social media was very problematic as well. While we would usually see social media as democratising information flows, the state did not. He gave the example of what the Mumbai Police which had recently set up the first Social Media Lab in India. The lab is staffed by constables and police officers who have never themselves used social medi. It requires them to monitor channels including Twitter and Facebook, and relies greatly on algorithms. He did not view these efforts as effective, pointing out that despite so much effort, they had not even been identify the owner of a popular ISIS Twitter handle as a young boy from Bengaluru.

Mr. Datta explained that data surveillance is becoming increasingly used because of the inefficiency of our intelligence and law enforcement agencies. He argued that a common pattern that one would encounter was that these agencies would adjust for their inability to execute effective, targeted surveillance by progressively increasing the levels of scrutiny of citizens' lives through mass surveillance in order to ensure that more and more data is available to them. He pointed out that this enthusiasm for data collection was not tempered by the realisation that this would create a tsunami of data coming their way, so that they would be able to do even less as their systems would slow down. Overall, he opined that the State's approach is to keep collecting data and use it for whatever purposes they choose, lawful or otherwise.

Mr. Datta then discussed recent instances of surveillance. He said that in the recent case of the terrorist attack in France, it was apparent that despite all the data collection by the National Security Agency, the French intelligence and the Government Communications Headquarters (GCHQ), there had been no prediction or prevention of the attack. He said that it was the same with the 9/11 terrorist attack in the United States. As regards the 26/11 Mumbai attacks, he noted that every study had shown that the necessary information was already recorded in the system, but because the State had been overwhelmed by the volume of data at its disposal and so had been unable to identify or use the information effectively.

Mr. Datta also said that political processes had totally failed to protect citizens and to ensure their privacy, and that this was a feature throughout our history. He emphasized that it was necessary to consider how the State views its citizens. To illustrate, he described India's Cyber Security Policy which made no references to privacy. Similarly, he noted that in the mid 1990's, it had been correctly predicted that the United States Congress would do very little to protect privacy, as the Snowden affair had made clear. He expressed disappointment that this was happening in India as well. He also mentioned the outrage following the German Chancellor's phone being tapped, and the recent revelation that the German intelligence had worked hand in hand with the National Security Agency doing the same thing to others.

Concluding his talk, Mr. Datta said that we must also carefully consider where databasing, and this increasing tendency to data collection in India leads. He said that the intelligence community's argument that they are looking for a needle in a haystack was an illogical one. He

argued that it was hardly logical to continue thoughtlessly increasing the number of haystacks or even the number of practically indistinguishable needles, if that was the aim.

Mr. Bhairav Acharya, Lawyer, Supreme Court of India and Advisor, Centre for Internet and Society, Bengaluru was the fourth and the last panellist on Panel – I.

He started by saying that he had two broad points to make regarding Indian surveillance law, but that in order to make them it was necessary to first provide a very broad outline of the Indian law on surveillance. He said that privacy has many aspects and is regulated differently in respect of each of those aspects, and in a variety of ways in India and other common law jurisdictions. So, for instance, the law responds differently to territorial privacy as it does to bodily privacy and so on. Therefore, one must not make the mistake of conflating privacy only with communication surveillance – the former has been a much larger and older concern.

He said that with regard to communications, the law in India is of colonial origin. There are two statutes in the late 1800's: The Indian Telegraph Act, 1885 and the Indian Post Office Act, 1889. Section 5(2) of the Indian Telegraph Act, 1885 creates a wiretapping empowerment and Section 26 of the Indian Post Office Act, 1889 also has a broadly comparable power in respect of the interception of letters. He noted that the interception of posts had been a very controversial topic in the 1950's, 60's and 80's, but was now dead. He saw this as ironic, as there was still little clarity about how courier services should be treated.

The Indian Post Office Act, 1889 was reviewed by the Law Commission in 1968. Mr. Acharya nited that this review was instructive because the interception power granted under the Indian Post Office Act, 1889 is almost exactly the same as the interception power under the Indian Telegraph Act, 1885. He said that subsequently however, a number of cases have not explicitly but by omission accepted what is a problematic wiretapping empowerment to begin with.

He thereafter very broadly reviewed the constitutional cases.

In India, the legal position in relation to privacy is muddled, and there are a lot of gaps. Mr. Acharya noted that the available law is presented in a textbook narrative of five or six cases that uphold the right to privacy. He argued that this was not an accurate characterisation.

He said that the first case that looked at privacy was the case of *Kharak Singh v. State of Uttar Pradesh*[1] in 1963, which every book and article would say is a foundational case. He did not however see this as being the case. The majority view in *Kharak Singh* held that only entry into a home at night might offer a claim of an invasion into privacy. It also found that if the impugned empowerment provision had been made by an Act of Parliament instead of through executive power, it would have been constitutional. He pointed out that *Kharak Singh* is cited for the Justice Subba Rao's dissent, which while certainly inspiring, lacked something that all good dissents have – an alternative test, or device by which to measure whether there was a privacy claim.

He said that the absence of a test to determine the chilling effects of invasions of privacy had failed India. India has not been able to devise its version of an already flawed reasonable expectations test because there was nothing in our precedent to go back to. He emphasised that this dissent makes the foundational moral claim to privacy in India, but noted that it is an incomplete one.

He made clear at this stage that there are three or four theoretical justifications for privacy. There is first, a classical liberal conception of the division between the public and the private sphere. This comes out of a very long and contested history of modernity. Hannah Arendt, for instance, in *The Human Condition* talks about this very eloquently saying that that which is private is that which naturally flows or naturally falls within the family, the home and so on. He also said that there is a lot of criticism of this conception, and that the most obvious feminist criticism is that if the home and the domestic life was shielded from the gaze of the law, then it might be excusing abuse.

There is also the right to be let alone conception of privacy which was formulated by Samuel Warren and Louis Brandeis in a very celebrated law review article in 1890. He saw the right to be let alone article as very interesting because both of India's foundational case laws on privacy make reference to it. He said, however, that the right to be let alone article while no doubt seminal and forward-looking for its time, was also incomplete. It fails to provide a theoretical framework for privacy – How does one measure this right to be let alone? How does one enforce

[1] AIR 1963 SC 1295.

it? How far does this right extend? Does it extend to the property? Does it extend to the body? Does it extend to the individual's decisions? The Warren-Brandeis formulation did not address any of these questions. He was of the view that the right to be let alone argument would make sense being put forward by two Americans given the political philosophy of the American State and its particular history of libertarianism. However, he pointed out that is not the history that Indians share. The State has never been remote from Indian society or economy for around the last sixty or seventy years, although that debate is changing now. He said that for these sixty or seventy years, citizens of India have demanded that the State intervene. Another criticism to the right to be let alone argument was that the privacy claim was not, in the real sense, a right to be let alone but rather a call for positive State interference to protect privacy. He said that in a developing country, this is a very important point to note, and that while Samuel Warren and Louis Brandeis could not be faulted for no recognizing this, the Indian Courts definitely could.

Thereafter, he moved to the second landmark case on the right to privacy – *Gobind v. State of Madhya Pradesh*[2]. He said that some say that this is the case that provided for the right to privacy in India but that he did not agree to this, though this case had the advantage of the personal autonomy jurisprudence which protected decisional privacy in the United States. He referred to the last two or three paragraphs in *Gobind* which said that if there is a case for privacy, it is subject to compelling State interests. This judgment failed to devise a test for what such a compelling State interest would be. He said that *Gobind* tied in very neatly to a national security oriented approach. He noted the lack of a definition and the lack of judicial understanding about what national security means. He said that security would always trump privacy if the terms compelling State interest was applied, without any definition.

Mr. Acharya then went on to discuss *People's Union for Civil Liberties v. Union of India*[3]. He thought that the judgment starts very promisingly by saying that telephone tapping is an invasion of privacy, but unlike the American case law, this judgment offers no test for determining what sort of communications should be protected. He raised the question of why telephone calls were included when e-mails, which did exist in 1996, were not. He acknowledged that in 1996, the

[2] AIR 1975 SC 1378.
[3] AIR 1997 SC 568.

Information Technology Act, 2000 had not yet been passed, and the Indian Telegraph Act, 1885 only applied to wired communication. He asked why the judgment did not hold that wireless communication should also be treated as private. He was of the view that the lack of judicial clarity was very problematic in this regard.

Against this backdrop, he presented four points on how Indian Courts have responded to surveillance and privacy claims. His first point was that there has been a complete lack of jurisprudential or theoretical clarity on what one can ground a privacy claim upon. *Gobind*, for instance, saw the Court go in three different directions. It first made a reference to the right to be let alone, which is an argument which calls for the State to be remote and distant. It then made a reference to the spatial concept of privacy by making a reference to the American case of *Olmstead*, which dealt with privacy in terms of territory. It also talked about the decisional aspects of privacy. That case's treatment of privacy as decisional autonomy stretched to its logical end would permit for instance a privacy claim to protect all forms of decisional autonomy including, for example, sexual or dress choices. *Gobind* did not do stretch this far, and therefore, was only a selective application of that law.

Nevertheless, despite this confusion, *Gobind* retained the public private divide. The Court expressly stated that privacy should naturally protect motherhood, the family, procreation and so on. Mr. Acharya, however, argued that privacy should go further, and protect actions outside marriage and the family, to protect some non-procreative activities as well. This, in his view, was a jurisprudential and a theoretical failure in *Gobind*, though he did not think it to be deliberate.

He then discussed *R. Rajgopal v. State of Tamil Nadu*[4] from the early 1990's. The case was quite confusing and dealt with privacy and press freedom. It held that ordinary people have a constitutional right to privacy as against the press. Despite the Court's application of a fundamental right, he pointed out that there was no State activity involved. He asked why Justice Jeevan Reddy should have reached for the right to privacy. He argued that the consequence of having done so was a conflation of the public private distinction. He argued that if one goes forward to claim of right to privacy, then one would need to be clear on where this claim finds its basis. Should it be based on a classical liberal model of privacy? Should it be based on sort of a

[4] AIR 1995 SC 264.

libertarian American idea of the right to be let alone which calls for a remote distant Government? Should it be based on a spatial claim, which means that one ultimately bases it on the law's propensity to protect private property – can this be done in a country like India?

He said that the second point in this respect was the absence of the exclusionary rule, *i.e.*, when evidence is collected from an unreasonable, illegal or improper search and seizure of private property, the evidence becomes inadmissible in Court. He explained that the United Kingdom which holds that if the evidence is *relevant* to the case, then the question of whether it was collected unlawfully or not is not required to be gone into. In 1914, the United States departed from this position establishing an exclusionary rule by which evidence that was improperly collected is not admissible in court. A series of decisions strengthened this rule in the American jurisprudence, so that the test is now a five step process.

In India, in 1972 the United Kingdom's position of considering releavance rather than manner of collection was adopted. On this point, Mr. Acharya discussed the Parliament attacks case from the 2000's – *State (NCT of Delhi) v. Navjot Sandhu*[5]. He specifically referred to paragraphs 148 to 154 dealing with the exclusionary rule. The wiretaps during investigation which yielded the incriminating evidence were all illegal. The Court held that the security was a competing interest that would trump privacy. He argued that this was a conflation of bad policing with national security concerns, and that it was very problematic for such reasoning to come from the Indian Supreme Court.

He said that there is also a question of the width of the Indian Executive power. Broadly speaking, in a democracy which separates power between the three branches of Government – the Executive, the Legislature and the Judiciary, the Executive power is the ability of the Centre as in India's case the Central Government and the State Governments to legislate without statutory action.

There are different kinds of Executive power.

First, there is the wider Executive power which the Centre can exercise even in the absence of a controlling law. This means that if one of the entries in our Union List gives the Centre the

[5] AIR 2005 SC 3820.

power to do certain things such as for defence or for the security of the State, then, even in the absence of a law of Parliament, it can take action. Second, there is a narrow power which is tightly circumscribed by a parent statute. In the context of the Information Technology Act, 2000, many of the Rules under it have failed on this count. They have been issued without the parent statute empowering the Executive to do so. He pointed out that it is a foundational rule since 1955 that the wider power of the Centre to legislate cannot bypass a statutory regime and that this has been totally ignored in India. As a result, he argued that the Rules framed under the Information Technology Act, 2000, which provide for content interception and traffic data collection, this foundational constitutional principle.

He then moved on to make the broader point concerning the entrenchment of governmentality. He explained that governmentality and bio-power are both concepts that Focault proposed and popularised. Governmentality is broadly the tendency of a nation state to co-opt its institutions, democracy and ultimately civil society into the government. He said that this is exactly what is happening with India. With the rise of the national security narrative, the Government has co-opted India's civil society and to a large degree its judiciary, so that outcomes in the major terrorism trial of India the Indian Supreme Court said that although the entire electronic part of the investigation seemed to have been illegally conducted, security is more important. The other important idea that Focault had talked about is bio-power which directly relates to the need of the nation state to have information about the bodies of its citizens. He said that this was the ultimate form of political power.

Mr. Acharya then discussed the impulses to privacy law.

The *first* comes from news media regulation, and is the oldest. The idea that privacy protects its citizens from an intrusive, sensationalist and rogue press is not new to Inda. Pandit Nehru and his good friend Manikonda Chalapathi Rau started a newspaper in 1937 called the *National Herald*. They were influenced by the experience of the *Manchester Guardian* and Harold Laski and Michael Foot and so on. When the first Press Commission Report came out, it had three broad recommendations. All three dealt with controlling the press and not encouraging it. The first was that there were press monopolies in India and it was the duty of the Government to break these monopolies because a monopolistic press could pose a challenge to the Government's attempts

to build a national narrative. He said that it must be understood that when India became independent, it inherited from the colonial Government an apparatus of censorship, the tools of censorship and the people to be controlled. Pandit Nehru sought to perpetuate this colonial approach. When they sought to break the press monopolies, he argued that they sought to break any challenge to the narrative of governmentality.

The Press Commission also discussed yellow journalism or sensationalism, which Mr. Acharya saw as subjective and open for debate. He noted that it incidentally is a question that is being raised now by the present Press Council. He said that there now there is a push of privacy that is coming from the people who want to see the press and media curtailed. There are calls being made for a media commission, for press censorship and for self regulation, and ironically many of these are coming from the Press Council itself. He then discussed the two major cases that deal with this. The first was the *Rajgopal* case from the early 1990's and the second was the ongoing *Ratan Tata* case which deals with privacy and the limits of press freedom, and the question of whether newspapers who innocently receive information from whistleblowers should publish it.

The *second* major push for privacy is coming from our information technology and outsourcing sector. He said that the entire Indian outsourcing model is based on receiving foreign information. India receives large amounts of data from Europe and America, and because Europe has strict data security laws which provide for privacy of European citizens' information, wherever processed, there have been calls for adoption of equal laws to protect this incoming data. In 2010, India had invited a data adequacy audit of Indian law, which it failed. In 2011, the Government did two things. It ordered the Department of Personnel and Training (DoPT) to start framing a new law, and at the same time, another Government department issued subordinate legislation in the form of Rules under the Information Technology Act, 2000. These Rules were India's first privacy law and they did not apply to Indians' information but to the foreign data coming in.

The *third* major push for privacy according to Mr. Acharya comes in response to State surveillance, which is being deeply contested in India. Ironically, he said that the regulation of State surveillance is the judicial basis of privacy protection. As flawed as the judgments in

Gobind and *Kharak Singh* were, they still laid the foundations for a later narrative on privacy. They did so because they were trying to regulate the limits of the State's ability to physically surveil the homes of Indian citizens.

Concluding his talk, he said that there is theoretical and intellectual confusion around privacy, but that there is a narrative that can be taken forward. However, in order for this to work the exclusionary rule must be strengthened – it would make no sense to regulate State surveillance if evidence which was unlawfully or improperly obtained was allowed by our courts in criminal trials. He said that if was condoned, then there would be no point in regulating State surveillance at all – what is the use of a wiretap law if an illegal wiretap can be used as evidence against an accused anyway?

He emphasised that India also needed to devise a privacy test. It would need to specify what privacy means in terms of communications. What sort of communications should be private? Why are they to be private? How does one signify privacy - Is it the intent to keep communications private? Is it the social recognition of privacy? Is it the mode of communication itself? Why is it that in India telephone calls, e-mails and letters are protected but not the other means of communication? Do some technologies of communication invite privacy?

He said that the last concern as regards privacy came from freedom from behaviour regulations – decisional privacy that would allow the exercise of personal autonomy in our choices. He said that this facet of privacy had received a great step forward in the in *Naz Foundation v. Govt. of NCT of Delhi*[6]. Even though the Supreme Court overturned the ruling, it did not explicitly negate the High Court's logic, so it is unclear if these arguments still stand.

Ending his talk, he said that decisional privacy is ultimately the only real marker of individual freedom and needs to be protected.

[6] 160 Delhi Law Times 277.

QUESTION AND ANSWER SESSION

Question [To Dr. Ramanathan]: Apart from the internet, if one talks about the Human Genome project, is that surveillance too?

Dr. Ramanathan said that the answer was yes. According to her, there are a lot of ambitions in science, but that there is no regulation surrounding it. This privileging of science is happening especially in the context of DNA, which is something which will have to be dealt with. She mentioned that there is a proposal to bring in a Human DNA Profiling Bill which will help scientists get into the Genome project but it will leave many people quite unprotected especially because it intends to create a database along with getting into these projects.

Mr. Raman Jit Singh Chima sought a clarification asking whether by the Genome project dealt with genetics specifically? He said the reason why he asked so was that in his view the Human Genome project by itself has been a fantastically positive thing and it had concluded in 2003.

Dr. Ramanathan replied that the main effort was the Human Genome Diversity project and that there are multiple others that involve similar concerns. For example, in the Human Genome Diversity project, whole databases have been moved and placed within the project as it has become easy for digitisation and carrying the data with them. There has been no question of taking consent, the universities haven't asked any questions about it and the professors conducting the research have moved and carried the data with them. She saw a number of issues raised by this state of affairs, but felt that most had even been touched. She said that under its earlier avatar, they had around 38 people just outside Madurai who were thought to have African roots – there is nothing to indicate that they had been told what their information was being given for, let alone why it had originally been taken in connection with a local project but then fed into the international project by the scientist. She pointed out that there are no norms to govern the scientist's work, and in their absence he did what he thought was best in that context. But it means that those 38 people had not consented and had no idea in what ways this information was going to be used.

Question [To Mr. Acharya]: Mr. Chima asked two questions. The first was on the specific point that Mr. Acharya had made about the Indian Telegraph Act, 1885 and privileging certain forms

of communication: when it comes to the Indian Telegraph Act, 1885 itself, doesn't the *PUCL* ruling apply to essentially all communication in telegraphic form? The definition in the Indian Telegraph Act, 1885 essentially is that anything that is wireline or wireless is covered, and so it would seems that this judgment applies to all forms of communication. The second was on the 43A regulations on data protection in regards to which Mr. Acharya had said that it applied to foreign players only. He asked about the effect of the Indian Government's press release in the latter half of 2011.

Mr. Acharya replied by saying that that though the Indian Telegraph Act, 1885 was enacted very early on, it applies to telephones and other forms of wireless and wireline communications. What he thought Justice Kuldeep Singh failed to do was ask what forms of personal communications between two people should be protected. The wiretap provisions particularly were challenged but it failed to devise a test that would ask questions as regards the nature of the communication more than the mode of communication. In 1996, when this judgment was delivered, e-mail was being used in India. Therefore, as of this judgment, it protected wired or wireless communications but not e-mail. What he meant by the lack of a test was an example of what he thought might have been a question that could well have been answered. This was the *Olmstead* question from 1928: what forms of communication should be protected and why, and what is the basis of this protection? In *Olmstead*, the United States Supreme Court held that a telephone call was not subject to the Fourth Amendment privacy claim because the call left the private property of the home and traveled on wires that traversed over public property. So, this is a very spacial and a territorial idea of privacy which one may agree or disagree with but its logical. He said that the *PUCL* case failed to introduce any real logic. The only test that the case did talk about was that to see if it is clearly the intent of two parties who talk to have their conversation private. According to him, this intent was not clear. But he pointed out that the intent had to be proved by a test. All privacy tests have an element of objectivity and subjectivity. In the United States Reasonable Expectation Test, the element of objectivity is introduced by asking the society to recognise as to what form of communication is private and the subjectivity is introduced by asking the person as to did he or she display an intent to demonstrate privacy. *PUCL* did not ask this. The absolute non consideration of these questions is what weakens this judgment. He said that though it was an extremely valuable judgment, it could have done a lot more.

Thereafter, he answered the second question raised by Mr. Chima on the 43A Rules. He said that there was an absolute lack of an appreciation for the width of the executive power by the state. When the 43A Rules were issued, they were so badly drafted that people couldn't figure out what they meant. Law firms shot off questions at the department in-charge, and the government responded with the press release. He said that putting all this aside, the point that he was trying to make was that if the data of certain individuals was to be protected then this should have been defined in the parent Act and in the Rules and should have traced to an executive empowerment given by the parent statute, in the absence of which it should have been made in conformity with the 1955 foundational case law on what one could do with subordinate legislation. These rules according to him did neither.

Comment [in regards to Mr. Acharya's talk]: Dr. Ramanathan commented on the judgment in the case of *Navjot Sandhu*. He mentioned that the papragraphs which Mr. Acharya referred to had been overruled in a recent decision by the Supreme Court in the case of *Anwar v. Bashir*. She further said that what bothered many people was that Afzal Guru was hanged on the basis of a decision then that was illegal and wrongly made, and that this is more serious than anything else that she could think of.

Mr. Acharya said that the judgment in the *Anwar* case was very welcome but that it is quite problematic in many ways. The case dealt with was that the widespread practice in the Indian Courts of adducing electronic evidence supported by an affidavit. He explained the wiretap process in this context. It is a three step process, where authorisation notionally comes from the Home Secretary. Then, it flows through a police officer who hands this order over to a Telephone Services Provider (TSP). The TSP is required by the licensing law to have a Nodal Officer who is personally responsible for the content of the wiretap. A tap is made, it is recorded onto a Compact Disc (CD). The Nodal Officer and the CD together go to Court, where and the Nodal Officer swears to the accuracy of the CD's contents. He said that this was a very simple way by which we completely side-step the hearsay rule. This had allowed a lot of evidence to be adduced in Courts, which Courts themselves just simply could not affirm the veracity of. So, the judgment in the case of *Anwar* was an attempt by Chief Justice R.M. Lodha and Justice R.F. Nariman to make sense of this because there are already provisions in the Indian Evidence Act,

1872 to deal with this. He said that all this judgment did was return the evidence procedure away from 65 and back to 65B.

He disagreed with Dr. Ramanathan that this judgment overruled the paragraphs he had cited in *Navjot Sandhu*. What it did do in order to avoid future confusion was that it held that electronic evidence must be certified. He argued that it did not overrule the relevant paragraphs because if it had done so it would have established an exclusionary rule which it did not do clearly. It would have said that wiretapping evidence which was wrongly taken should not be admissible. All it did do was alter the procedure – it did not say that the certification had to speak to the fact that the evidence was properly obtained. The certifier of electronic evidence under the Information Technology Act, 2000 is just supposed to certify four or five conditions – that the machine was working, that it did its proper purpose and so on. This authority is not supposed to look into whether the evidence has been properly obtained. So notionally one can still illegally wiretap, and have the CD containing the result duly certified.

Question: [To Dr. Ramanathan] A student of social sciences at the Jawaharlal Nehru University, Delhi said that what has happened over the years in her University is that there is a growing demand for Closed Circuit Televisions (CCTVs) because apparently there being laptop thefts, etc. The Students' Union in her University has so far successfully resisted CCTVs at certain locations, the campus remained fairly safe. But what is being pushed right now is a Radio Frequency Identification (RFID) system in the library students fear that if someone issues a book out of the library and then goes to a protest at Jantar Mantar, for example, his or her location can be tracked. She said that they do not know how to deal with this or how to resist this because apparently there is a lot of push from the service provider who was vying for what would be a multi-crore project. She asked Dr. Ramanathan if she had any thoughts about this.

Due to the paucity of time, Dr. Ramanathan replied on a light note that she would come to her University and respond to this.

Comment [Generally]: Professor (Dr.) Shulz then said that he would like to share two points that the panellists might comment on. The first thing was that people from legal studies and policy makers pretend to try to find solutions or design norms and maybe the perspective should be broadened and technical solutions, for instance ,should be looked at. He said that when Professor

Park talked about RRNs, a solution might be that trust of a party is gained so that it translates these numbers into different other numbers which can be used in different contexts so that in different databases, there exist numbers that can identify a specific person rather than having the same numbers in all databases. So, identity thefts for example might at least be not easy as it is now.

He said that the second point was that when the problems in framing what privacy really is and different aspects of privacy were being talked about, a solution might be to have a project involving different jurisdictions and bringing together all their perspectives to make the debates in India or elsewhere more rational. He said that for instance there is a Supreme Court decision in Germany where they at least try to differentiate different types of threats and say only when this type of imminent danger is really to be proven then surveillance is lawful.

Questions [To Mr. Datta, Mr. Acharya and Generally]: Thereafter, Mr. Pranesh Prakash raised three points.

The first one was to Mr. Datta about the numbers on surveillance. He said that he had been hunting them down and asked where Mr. Datta had courced his figure of 100, 000. from because he could find a one hundred and fifty one thousand over a five year period that reliance revealed before the Supreme Court in a case and said that there is another number of ten thousand which came from a press release by the Cabinet Secretariat about how many were being ordered by the Central Government and that was for a one year period. However, he admitted that he could not find any information beyond that.

The second question was to Mr. Acharya: why did he want theoretical purity? Couldn't privacy be thought of as having different jurisprudential basis all bundled together?

His final question was for the larger panel: how could the current situation of privacy which had been talked about be changed? At least the Centre for Public Interest Litigation (CPIL) has filed one Public Interest Litigation (PIL) in the Supreme Court for intelligence agencies to have a basis in statute. He said that this perhaps might be useful, but he was not very positive given that since atleast the 1980's, there have been multiple cases of politicians being targeted by iunlawful surveillance and nothing had changed. He also mentioned that there have been instances like in

Himachal Pradesh, where more than one thousand unlawful intercepts have been ordered. The uncovering of this in 2012 did not make headlines, the story was covered in the inner pages of two or three different newspapers and that was it. In Gujarat, it was found that ninety thousand illegal requests had been made over a one year period for call data records, and that didn't make headlines either. He asked how people's concern for communications privacy in India could be aroused.

Responding first, Mr. Acharya said that he didn't want theoretical purity. He was calling for Indian Courts to have theoretical clarity on the issue. He said *Gobind* was a total mishmash of theory which didn't really make for a convincing argument. He said that he did not want a national claim or a cultural claim of privacy to be based on a particular theory. What he wanted was that the Indian Courts and the Indian lawyers have theoretical clarity.

Thereafter, Mr. Datta responded to Mr. Prakash. His figure of 100,000 came in a response to a Right To Information application which was made to the Home Ministry.

On the point that Professor (Dr.) Schulz had made about the Supreme Court and setting the rules etc., he said that under Rule 419A there existed certain conditions under which interception can be allowed but the basic framework is faulty and problematic because there is no data to show under what circumstances they are actually being used unless there is a leak, because the framework does not provide for judicial or political intervention.

Thereafter, Mr. Datta proceeded to respond Mr. Prakash's questions to the larger panel. He said that various systems, for instance, the Foreign Intelligence Surveillance Act, 1978 and the Courts it created in the United States of America have failed as Edward Snowden has clearly revealed. Just having political oversight in addition with the judicial oversight would not work. The only way to his mind was by ensuring a statutory regime for transparency, under which if somebody is targeted for surveillance, the product of the effort should either be taken to a Court of law and be introduced as evidence in a prosecution or the person must be informed that he or she was under surveillance. He said that the day India has that kind of a regime, the State will immediately start tightening up its systems.

Comment [Generally]: Dr. Ramanathan next said that she was part of a discussion in the privacy committee, where it was said that if anybody is put under surveillance then at some stage maybe six months after the surveillance having ceased or three years from when the surveillance began, the person should be informed that he or she had been placed under surveillance. She said that such person had a right to know. She informed the room that this had been strongly resisted to within.

She had expressed disbelief that there are 100,000 supposed terrorists under surveillance.

In response to the question posed earlier by the participant from Jawaharlal Nehru University, Dr. Ramanathan said that though she had earlier said that she would come to the University and talk about this, she wanted to reiterate one point and said that that very often there is this idea that when there is a problem this is a solution. CCTV, in her view, was a classic case of how the so called solution is itself the problem. She asked that this be considered in light of the kind of relationship that everyone has with the police – in police stations there would be monitors which looking at where one stands, to whom he or she talks to, where one gets on to a bus, how far one travels and how often does one do that day after day after day – all without us having any ability to protect this data. She said that this being offered as a service for the people to be safe is a clear case of how absurd some solutions can be because they in fact create bigger problems.

On Mr. Prakash's question as to how to get people interested, if something as big as this is not even a dot in the newspapers, then there is really some matter in the way people view it and the idea of privacy seems to have not captured in the people's imagination. She said we would need to cast privacy as individual security, as operational security, as security from the people who are looking at others, and maybe play up this imagination a little bit. She said that recognising that a lot of this deliberate dilution of the idea of privacy is coming because there are multiple agencies who want to able to watch people, and who would therefore teach the people how to disregard privacy by offering a number of other things in its place. She said that she must confess that today she felt much less secure than she did when all these things were not around.

Adding to this, Mr. Datta made a final point saying that there was also a problem because surveillance today has become a multi-billion probably a multi-trillion dollar industry and these

companies are pushing Governments to increase their ways of surveillance, etc., so push back against that is becoming increasingly difficult because huge businesses are dependent on that.

PANEL II: UNPACKING THE INTERMEDIARY LIABILITY DEBATE IN INDIA

Professor (Dr.) Wolfgang Schulz, Director, Alexander von Humboldt Institute for Internet and Society was the first panellist on Panel - II.

He started by referring to the judgment of the European Court of Justice in the *Mario Costeja González*[7] case. Summarizing the facts, he said that Mr. Costeja González, a Spanish national, filed a complaint against the data protection officer in Spain. Mr. Gonzales wanted a newspaper, which had reported a case involving him (where he was forced to sell his property) to take it down from its online database. At the same time, he claimed that Google should remove the link to this content from its search results as well. This case went to the European Court of Justice and Mr. Costeja González was successful. He noted the irony of the fact the only thing most people knew about Mr. Costeja González was the very fact that he had worked so hard to have suppressed.

Prof Schulz explained that the European Court of Justice did three things:

First, the Court held that jurisdiction would arise where the money is being earned and where the data been processed. In this case, Spain was held to have jurisdiction.

Second, the Court held that search engines are not just intermediaries but data controllers for the purposes of the European data protection regulation and are therefore responsible for the data.

Third, when one inserts the name of an individual, the production of a list of links is an act covered by the European data protection regulation. The effect of the ruling is that an individual can claim that data in these lists should be deleted when he or she feels it infringes on his or her privacy.

Prof Schulz noted that Internet had been in uproar when this decision was announced. The criticism was that when something is available on the Internet legally to start with, it cannot be

[7] *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González*, Case C-131/12 (Court of Justice of the European Union).

illegal to make it available on search engines. He saw merit to this argument but thought that it lacked precision.

Prof Schulz then briefly discussed four points:

The *first* point was that when a proper system of Internet intermediary governance and liability is discussed, one has to understand the specific function of the intermediary in question to make a proper decision. In his view, the European Court of Justice was right on the first level but wrong on the second. The first level is that the function of search is, to some extent, to draw attention to content, and search engines give an ordered list of links that provide information in response to a specific query. This means that they create a specific kind of publicity. In his view, the ECJ had correctly said as much. So, the argument that a given piece of content is legal on the Internet so it must be legal for an online intermediary to give access to that is too simple.

The *second* point was that it is assumed that there is a kind of public sphere created by search engines. When we want to know about a person, we use a search engine into which the name is typed in and through which links are accessed so as to create a specific public sphere around the subject of the query. Prof Schulz argued that the instruments of data protection under the regulation are not adequate because when one talks about public spheres, then he or she also talks about public interest in this person and the interests of this person to have influence over his or her image in that public sphere. He said that he believed that all those questions of intermediary liability when it comes to cases like this should not be dealt with by data protection law but by the laws differently that systems have devised for instance, when it comes to press or media coverage of a person. He argued that what different intermediaries really do, that is to say what social functions they have, has to be carefully understood before an effective system can be designed.

Third, Prof Schulz argued that the fundamental rights aspect of intermediary liability is often neglected. He said that the problem in intervening at the point of intermediaries is that, as a rule, there is one interest that is represented really strongly, that is to say, for example, a copyright holder sees that there might be an infringement and files a claim therein as it affects his or her rights therein. He noted that all parties did not have a symmetry of resources in these cases. An intermediary would therefore be likely have an easy decision to say that if it might run into

liability risk then it would simply remove the content from its search results or its social media platform. He saw serious right to information and freedom of speech concerns because these types of situations can create a system where legal claims on the internet would not be found, as intermediaries decide, within the liability system, to remove content rather than carry the risk of litigation. So, Google, which can afford to create its own system, has created a mechanism where it decides whether it wants to remove the link or not. Other search engines gave people the opportunity to initiate a process after which links are removed. As a result, he argued that there is a real need to consider the fundamental rights dimension.

Relatedly, he emphasized that in order to usefully understand intermediary governance, the whole picture (and not only the rules that the Government has enacted to regulate liability) must be considered. In particular, he argued that we must carefully consider what incentives are created for an intermediary to act in favour of free expression.

Finally, Prof Schulz turned to the consequences of the ECJ's decision. Reading between the lines shows that the Court wanted to send a signal against powerful companies like Google. He pointed out that, in effect, the ECJ had created a system where an intermediary actively decides about third party liability in conflict.

Concluding his presentation, Prof Schulz mentioned the Network of Centres' work on Internet intermediaries' liability in different countries. He explained that its object was was to make a starting point for mutual learning, where law makers, self regulators, intermediaries themselves, and whoever was involved in this system could see what other models exist and what unintended consequences specific instruments can have.

Ms. Chinmayi Arun, Research Director, Centre for Communication Governance, National Law University, Delhi was the second panelist on Panel - II.

She started by framing what the NoC India Country Report had done and outlining what the remaining panelists would be discussing. She mentioned that an India Country Report had been drafted as a part of the study which Prof Schulz had described. She said that it tried to map the intermediary liability system in India and analyse its consequences.

As the report explained in greater detail, she explained that a licensing system covers access intermediaries such as Internet Service Providers (ISPs) and telecom companies. A number of issues that the previous panel had discussed in the context of surveillance tied into the contents of these licenses: requirements that get ISPs to co-operate, to hand over the data to the Government, and which permit the Government to run searches through large amounts of data, come from their licenses. Similarly, requirements to block certain kinds of content could also come from the licensing obligations. She noted that online content providers and web based platforms like Google, Facebook and Twitter are also subject to these requirements.

She placed the obligations imposed on intermediaries in India into three categories: blocking, interception and takedowns.

Ms. Arun then discussed the notice and the takedown regime under which anybody could send an intermediary a notice alleging that content is illegal and expect it to be taken down. She said that as Prof Schulz had correctly pointed out, this liability can be used in multiple ways to regulate intermediaries in India. She explained that intermediaries act as gatekeepers for information online, and blocking, interception and takedowns involve the Government trying to control the flow of information, to gain access to it or to influence it in a particular ways using the middle man.

Mr. Sarvjeet Singh, Project Manager and Research Fellow, Centre for Communication Governance, National Law University, Delhi was the third panellist on Panel - II.

He discussed the manner in which blocking operates in India. He started by briefly discussing Government ordered blocking. He said that such blocking raises a number of concerns, including around the right to a neutral inquiry, due process in terms of a hearing being provided to the owner of the content and the issue of transparency.

He then discussed the procedure itself. Government ordered blocking of content takes place under Section 69A of the Information Technology Act, 2000. The Act provides that if the Government – appointed officer is satisfied that the blocking request received from the different Ministries and the various State Departments falls under one of the grounds provided under Section 69A, and that it is necessary, an order for blocking can be passed. The grounds which are

provided for under Section 69A include sovereignty and integrity of India, security of the state, friendly relations with foreign states and so on. These terms broadly mirror all the terms that are provided under Article 19(2) of the Constitution of India, except that under Section 69A, there is a new term that has been inserted – the defence of the State. No definition of what this term means has been provided.

The procedure for blocking is further contained in a piece of delegated legislation known as the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009. These Rules provide for three broad categories of blocking. The first is executive blocking, the second is blocking in cases of emergency, and the third is blocking through Court orders.

He said that broadly the Rules that provide for blocking state that intermediaries must comply with requests for blocking which are sent to them by the Designated Officer under the rules. Under these Rules and the Information Technology Act, 2000, the Designated Officer is the only person who can order blocking. He then discussed penalties, noting that if intermediaries do not comply with blocking orders, they can be imprisoned for periods of upto seven years and also face a fine.

He also said that the process through which this blocking takes place is highly problematic as there are very few external checks and balances during its different stages. Basically, these Rules provide for the review of requests for blocking by different committees. All these committees consist of members of the Executive alone – there is no judicial or other independent oversight. These Rules also do not provide for notice to the owner of the content, and notice is only provided to the host, which in most cases will be the intermediary itself.

He opined that Rule 16, which provides that all these orders have to be confidential, and no information regarding them can be provided to the public, made matters considerably worse. He found this state of affairs especially concerning, arguing that what this does is that it makes the entire process very opaque, and a normal citizen has no information about what content is being blocked and so has no opportunity to challenge the blocking before a Court of law.

Ms. Arun then resumed, saying that as *Mr. Singh* had pointed out, there is serious transparency and accountability problem with the blocking process as it works in India. The Government does not notify when it is blocking content. It prohibits service providers, whether it is online intermediaries, web based platforms or Internet service providers from telling content owners the when they are blocking. If one files a Right to Information request, he or she is told that Rule 16 does not permit the revelation of this data. The only way in which the number of instances of blocking in India for a given time period was for a Member of Parliament ask a question in Parliament. She mentioned that this was where CCG had got their data for the Freedom on the Net India Country Report.

She said that this creates a very serious problem because ordinarily if one finds that the law has resulted in speech being restricted in a particular way, it is open for the speaker to challenge this in Court arguing that his or her speech is protected by Article 19(1)(a) of the Constitution of India, and the manner in which it has been restricted does not fall within the reasonable restrictions under Article 19(2). She said that in the present situation, this cannot be done because one does not have the necessary information. In fact, one does not even know whether it is blocked by the Government or by an intermediary acting in the capacity of a private party. In the latter case, the owner of the blocked content does not have any rights in regard to this against a private party. She opined that this system creates very serious freedom of expression issues.

She then discussed the process by which the blocking orders are presented to a Review Committee. The Review Committee is supposed to be look at all the Universal Resource Locators (URLs) that are blocked, but it appears from the number of URLs that are blocked that this is quite difficult. Additionally, there is also the question of how the Review Committee accesses this content to determine whether this is content which ought to be blocked in India if these URLs have already been blocked and are therefore inaccessible. Ms. Arun saw this as an interesting paradox.

Concluding her talk, she said that in India, a safe harbour protection is provided to intermediaries under the Information Technology Act, 2000. This means that if one is an intermediary that is merely a platform or that just routes content but it doesn't apply mind to it, it has a protection

against liability for content. She referred to the *Bazee.com*[8] case, in which an explicitly sexual video of two minors found its way onto a web auction website, Baazee.com, raised the question of whether an e-commerce website could be held responsible for obscene content posted on it. After this, the Indian law was changed to make sure that intermediaries which do not apply their minds to the content are not ordinarily liable. The protection that is available to them is, however, conditional on as due diligence. Ms. Arun explained that this requirement for 'due diligence' was inserted on the insistence of the Parliamentary Standing Committee, and it implied a positive obligation for intermediaries.

She ended by noting that when an intermediary receives a request for takedown, it has to decide whether to takedown the content or risk expensive litigation in the current framework. It will choose the latter.

Mr. Apar Gupta, Lawyer, Supreme Court of India and High Court of Delhi was the fourth panelist on Panel – II.

He opened by saying that it may be useful to look at Sections 95 and 96 of the Code of Criminal Procedure, 1973. These two sections contain provisions and powers available to State Governments to prohibit publications. They also prescribe certain safeguards which have been in place since the British Raj as Sections 99A and 99F under the Code of Criminal Procedure, 1898. He pointed out that they are not a direct outgrowth of the reasonable restrictions enumerated under Article 19(2) of the Constitution of India.

He said that if one looks at the blocking provisions and especially at how blocking orders are passed by the Executive, the criticism that principles of natural justice are not being complied with is often heard. The criticism is essentially that the author or the owner of the content is not given any notice and judicial scrutiny is not applied at any stage.

He said that a predominant proportion of the blocks are not due to executive orders, but can be traced to judicial orders. There is no role of the Government by itself in this class of blocks.

[8] *Avnish Bajaj v. State (NCT) of Delhi*, (2005) 3 CompLJ 364 Del.

There is a private party approaching the Court complaining of a legal injury. This legal injury will usually fall into two broad laws. The first is defamation and the second is copyright.

He said that defamation as a substantive injury has developed in India as a civil claim in common law and is not contained in statute. In other words, it has been developed case by case, and originates from Great Britain. Substantively, if one looks at how it is applied, then the determinations in defamation do lean towards providing exceptions to authors, but that is only when authors approach Courts and contest the case over the long period of time litigation draws out for in India. He pointed out that very few defendants would stick out their necks for ten to twelve years defending a book that is already inaccessible through the use of injunctions. He referred, by way of illustration, to *Kushwant Singh* v. *Maneka Gandhi*[9], in which an interim injunction was passed against Kushwant Singh. This was ultimately reversed on appeal, but it took eight to eleven years to overturn it. During this period, the book was not available for sale and Kushwant Singh had to carry the resulting financial injury.

In the context of websites, Mr. Gupta referred to *Nirmaljit Singh Narula v. Indijobs At Hubpages.Com*[10]. The plaintiff was a religious leader whose claims were being questioned in a way, which was allegedly defamatory on a blog which was hosted on an intermediary called Hub Pages. Hub Pages was a blogging platform, and the plaintiff alleged that after sending a notice to Hub Pages to takedown the content, they failed to do so within thirty six hours. He pointed out that the (unreported) interim order of the Court reveals that the reasoning of the Court proceeds on a mere reproduction of the plaint and scrutiny by the Court is severely lacking, so that the prima facie case is merely portions which are excerpted from the suit itself.

Mr. Gupta then moved on to cursorily discuss copyright law in India. He said that copyright law was much more complex, but that it does not provide for liability of intermediaries if it transiently or incidentally stores information. Liability only arises when storage is permanent. In orders under copyright law, he pointed out that there was atleast some notice of blocked content in the form of annexures to ex parte orders, which list the websites being blocked.

[9] AIR 2002 Delhi 58.
[10] CS (OS) 871/2012 (Delhi High Court).

Ending his talk, he said that we must all use our access to Court proceedings to force clarifications of legal standards.

Mr. Raman Jit Singh Chima, Lawyer was the last panelist on Panel - II.

He started on note that online intermediaries should not be called intermediaries but that they should be called speech engines. He pointed out that the Internet makes a lot of information discoverable. Many platforms in India help in making available Court judgments to citizens. He pointed out that under the current system of taking down content, it might also be that someone says that a speech engine should takedown a particular judgment from its platform as the name of the defendant in that judgment might be similar to his or her name. With respect to the blocking of websites, he said that such blocking was in vogue of and on since 1999 – much before the Rules that Mr. Singh had mentioned. He said that in 2004 or 2006 orders were issued by the Government to block websites. Government officials defended them by saying that this was not censorship. Lawyers speaking against these orders said that ministerial orders hold no force.

Mr. Chima then proceeded to introduce the cases pending the Supreme Court. He talked about a petition filed by Shreya Singhal in the Supreme Court in connection with arrests of two Mumbai girls in response to a *bandh* organized by a political party in Mumbai on account of the natural death of their leader. These girls had criticized the *bandh* on Facebook and were arrested for their comments. Mr. Chima noted that the second incident which had triggered the petition was an arrest in West Bengal for posting derogatory remarks against the state's Chief Minister.

He also discussed how the Union Government had issued guidelines for intermediaries, noting that they had opened the floodgates for many challenges to the intermediary liability regime at the Supreme Court, with petitions being filed w by many Indian NGOs and intermediaries including Common Cause, People's Union for Civil Liberties, the Internet and Mobile Association of India and Mouthshut.com. He explained that all of these petitions had been tagged to be heard together by Supreme Court.

He also mentioned a public interest litigation[11] filed in the Supreme Court seeking blocking of advertisements and the online web links relating to pre-natal sex determination in India which is illegal in India.

In conclusion, he noted that the *Shreya Singhal* case and the batch of petitions tagged with it were the first extensive judicial engagement with what content is acceptable and what is not online.

[11] *Sabu Mathew George v. Union of India*, WP(C) 341/2008 (Supreme Court).