THE ALL INDIA PRIVACY SYMPOSIUM

FEBRUARY 4TH 2012
9:30AM - 5:00PM

THE INDIAN INTERNATIONAL CENTRE, NEW DELHI

CONFERENCE REPORT

IDRC CRDI | CENTRE FOR LAW & POLICY RESEARCH | PRIVACY INTERNATIONAL | PRIVACY INDIA | SAG society in action group | internet & society | Commonwealth Human Rights Initiative

THE ALL INDIA PRIVACY SYMPOSIUM: A REPORT

Privacy India, the Centre for Internet and Society and Society in Action Group, with support from the International Development Research Centre, Privacy International and Commonwealth Human Rights Initiative organised the All India Privacy Symposium at the India International Centre in New Delhi, on February 4, 2012. The symposium was organized around five thematic panel discussions:

Panel I: Privacy and Transparency

Panel II: Privacy and E-Governance Initiatives

Panel III: Privacy and National Security

Panel IV: Privacy and Banking

Panel V: Privacy and Health

INTRODUCTION

Elonnai Hickok (Policy Advocate, Privacy India) introduced the objectives of Privacy India. The primary objectives were to raise national awareness about privacy, do an in-depth study of privacy in India and provide feedback on the proposed 'Right to Privacy' Bill. Privacy India has reviewed case laws, legislations, including the upcoming policy and conducted state-level privacy workshops and consultations across India in Kolkata, Bangalore, Ahmedabad, Guwahati, Chennai, and Mumbai. India like the rest of the world is answering some fundamental questions about the powers of the government and citizen's rights and complications that arise from emerging technologies. Through our research we have come to understand that privacy varies across cultures and contexts, and there is no one concept of privacy but instead several distinct core notions that serve as complex duties, claims and obligations.

PRIVACY AND TRANSPARENCY

Panelist	Ponnurangam K, (Assistant Professor, IIIT New Delhi),), Chitra Ahanthem (Journalist, Imphal), Nikhil Dey (Social & Political Activist), Deepak Maheshwari (Director, Corporate Affairs, Microsoft), Gus Hosein (Executive Director, Privacy International, UK), and Prashant Bhushan, (Senior Advocate, Supreme Court of India).
Moderator	Sunil Abraham (Executive Director, Centre for Internet and Society, Bangalore)
Poster	Srishti Goyal (Law Student, NUJS)

Srishti Goyal provided the general contours, privacy protections, limits to privacy and loopholes of policy relating to transparency and privacy, specifically analyzing the Right to Information Act, Public Interest Disclosures Act, and the Official Secrets Act.

Nikhil Dey commented on the interaction between the right to privacy and the right to information (RTI). He referred to Gopal Gandhi, the former Governor of West Bengal, "we must ensure that tools like the UID must help the citizen watch every move of government; not allow the

government watch every move of the citizen." Currently, the RTI and the UID stand on contrary sides of the information debate. A privacy law could allow for a backdoor to curb RTI. So, utmost care has to be taken while drafting legislation with respect to right to privacy.

Data and information has leaked furiously in India and it has leaked to the powerful. A person who is in a position of power can access private information irrespective of any laws in place to safeguard privacy. It is necessary to look at the power dynamics, which exists in the society before formulating legislation on right to privacy. According to Nikhil Dey, there should be different standards of privacy with respect to public servants. A citizen should be entitled to information related to funds, functions and functionaries. The main problem arises while defining the private space of a public servant or functionaries.

The RTI Act has failed to address the legal protection for the right to privacy. Perhaps, rules regarding privacy can be added to the Act. It can be defined by answering the questions: (i) what is 'personal information'? (ii) what is it's relation to public activity or public interest? (iii) what is the unwarranted invasion of the privacy of an individual? and (iv) what is the larger public good? Expanding on these four points can provide greater legal protection for the right to privacy.

Gus Hosein described the intersection and interaction of the right to information and the right to privacy. He referred to a petition filed by Privacy International requesting information on the expenses of members of parliament. Privacy and transparency of the government are compatible in the public interest. Gross abuse of the public funds by MPs was revealed by this particular petition such as pornography or cleaning of moats of MPs homes. Privacy advocates are supporters of RTI, however, it cannot be denied that there is no tension between transparency and privacy. In order chalk out the differences, there is a need of a legal framework. According to Gus Hosein, in many countries the government office that deals with right to information also deals with cases related to right to privacy.

Mumbai and New Delhi police have started using social media very aggressively, encouraging citizens to take photographs of traffic violations and upload them to Facebook or Twitter. In reference to this, Ponnurangam described the perceptions of privacy and if it agreed or conflicted with his research findings. Ponnurangam has empirically explored the awareness and perspective of privacy in India with respect to other countries. He conducted a privacy survey in Hyderabad, Chennai and Mumbai. People are very comfortable in posting pictures of others committing a traffic violation or running a red light. Ironically, many people have posted pictures of police officers committing a traffic violation such as not wearing a helmet or running a red light.

Chitra Ahanthem described the barriers and challenges of using RTI in Manipur. There are more than 40 armed militia groups, which are banned by the central and state government. The central government provides economic packages for the development of the north-east region. However, the state government officials and armed groups pocket the economic packages. These armed

groups have imposed a ban on RTI. Furthermore, Manipur is a very small community. If people try and access information through RTI they risk getting threatened by the Panchayat members and being ostracized from the community or their clan.

People are apprehensive about filing RTI because they believe that these procedures are costly and the police and government may also get involved. Officials use the privacy plea to avoid giving out information. Since certain information are private and not in the public domain, government officials, use the defense of privacy to hide information. In addition, the police brutality prevalent in the area deters people to even have interactions with government officials.

According to *Deepak Maheshwari*, the open data initiative is a subset within the larger context of open information. There is an onus on the government to publish information, which is in the public domain. As a result, one does not necessarily have to go through the entire process of filing an RTI to get information, which is already there in the public domain. Moreover, if it is freely available in public domain, then one can anonymously access such information; this further strengthens the privacy aspects of requesting information and facilitating anonymity with respect to access to such information in the public domain. It has also to be noted that it is not sufficient to put data out in the public domain but it should also disclose the basis of the data for example, if there is representation of a data on a pie chart, the data which was used to arrive at the pie chart should also be available in the public domain. The main intention of releasing data to the public domain or having open data standards should not only be to provide access to such data but also should be in such a fashion so as to enable people to use the data for multiple purposes.

Prashant Bhushan noted that one of the grounds for withholding information in the RTI Act is privacy. An RTI officer can disclose personal information if he feels that larger public interest warrants the disclosure, even if it is personal information, which has no relationship to public activity or interest. This raises the important question, "what constitutes personal information?" He referred to the Radia Tapes controversy. Ratan Tata has filed a petition in the Supreme Court on the grounds that the Nira Radia tapes contained personal information and that the release of these tapes into the public domain violated his privacy. The Centre for Public Interest Litigation has filed a counter petition on the grounds that the nature of the conversations was not personal but in relation to public activity. They were between a lobbyist and bureaucrats, journalists and ministers. Prashant Bhushan stressed the importance of releasing these tapes into the public domain to show glimpses of all kinds of fixing, deal-making and show how the whole ruling establishment functions. It is absurd for Ratan Tata to claim that this is an invasion of privacy. Lastly, he felt when drafting a privacy law, clearly defining and distinguishing personal information and public is extremely important.

One of the interesting comments made during the panel was on the assumption that data is transparent. Transparency can be staged; questions have to be asked around whether the word is itself transparent.

PRIVACY AND E-GOVERNANCE INITIATIVES

Panelist	Anant Maringanti, (Independent Social Researcher), Usha Ramanathan, (Advocate & Social Activist), Gus Hosein, (Executive Director, Privacy International, UK), Apar Gupta, (Advocate, Supreme Court of India), and Elida Kristine Undrum Jacobsen (Doctoral Researcher, The Peace Research Institute Oslo).
Moderator	Sudhir Krishnaswamy (Centre for Law and Policy Research)
Poster	Adrija Das (Law Student, NUJS)

Adrija Das discussed the legal provision relating to identity projects and e-governance initiatives in India. The objective of any e-governance project is to increase efficiency and accessibility of public services. However, a major problem that arises is the linkage of the data results in the creation of a central database, accessible by every department of the government. Furthermore, implementing data protection and security standards are very expensive.

Sudhir Krishnaswamy highlighted the default assumptions surrounding e-governance initiatives: e-governance initiatives solve governance problems, increase efficiency, increase transparency and increase accountability. It is important to analyze the problems that arise from e-governance initiatives, such as privacy.

Usha Ramanathan described the increased number and vastness of e-governance initiatives such as UID, NPR, IT Rules and NATGRID. There are also many burdens on privacy that emanate from the introduction and existence of electronic data management systems. Electronic data management systems have allowed state to collect, store and use personal information of individual. Currently, the DNA Profiling Bill is pending before the Parliament. It is important to question the purpose and need for the government to collect such personal information. It is also to be noted that, there are certain laws such as Collection of Statistics Act, 2008 that penalize individuals if they do not comply with the information requests of the government.

Anant Maringanti discussed the limitations of data sharing that once existed. Currently, data can move across space in a very short time. He analyzed the state and market rationalities involved in e-governance initiatives, which raise the question "who can access data and at what price?". Data may seem to be innocent or neutral, but data in the hands of wrong people becomes very crucial due to abuse and misuse. For example, Andhra Pradesh was praised as the model state for UID implementation. However, during the process of collecting data for UID a company bought personal information and sold the data to third parties.

Apar Gupta discussed the dilemmas of e-governance. Generally information in the form of an electronic record is presumed to be authentic. The data which government collects is most often inaccurate and wrong. So the digital identity of a person can be totally different from the real

identity of that particular person. The process for correcting such information is also very inconvenient and sometimes impossible.

Under the evidence law any electronic evidence is presumed to be authentic and admissible as evidence. The Bombay High Court decided a case involving the authenticity of a telephone bill generated by a machine. The judgment said that since it is being generated by a machine, through and automated process, there is no need to challenge the authenticity of the document, it is presumed to true and authentic. The main danger in such case is that one does away with the process of law and attaches certain sanctity to the electronic record and evidence.

It should be also observed that how government maintains secrecy as to the ways in which it collects data. For example, the Election Commission has refused to disclose the functioning and design of electronic voting machines. The reason given for such secrecy is that if such information is put in the public domain then the electronic voting machines will be vulnerable and can be tampered with. But we, who use the voting machines, will never find out its vulnerabilities.

According to *Gus Hosein*, politicians generally have this wrong notion that technology can solve complex administrative problems. Furthermore, the industry is complicit; they indulge in anti-competitive market practice to sell these technologies as a solution to problems. However, such technology does not solve any problems rather it gives rise to problems.

Huge amount of government funds is associated with collection of personal data but such data is rendered useless or rather misused, because the government does not have clue as to how to use the data for development and security purposes. The UK National Health Records project estimated to cost around twelve to twenty billion pounds. However, a survey carried out by a professor in University College London showed that the hospital and other health institutions do not use the information collected by the National Health Records. Similarly, the UK Identity Card scheme was estimated to cost 1.3 billion pounds and finally it was estimated to cost five billion pounds. The identity cards are rendered obsolete, the sole department interested in the identity card was the Home Office Department, no other department intended on using it.

Technology should be built in such a manner that it empowers the individual. Technology should allow the individual to control his identity and as well as access all kinds of information available to the government and private bodies on that individual.

According to *Elida Kristine Undrum Jacobsen*, technology is regarded in this linear manner. It is increasingly being naturalized and as an all-encompassing solution. The use of biometric systems in the UID raises three areas of concern: power, value and social relationships.

With regards to power, there is a difference between providing documentation and information for identification. However, problems arise when the mode of identification becomes one's body. It also

leads to absolute reliance on technology, if the machine says that this is an individual's identity then it is considered to be the absolute truth and it does not matter even if the individual is someone else. It becomes furthermore problematic with biometric system because it is generally used for forensic purposes.

The other component of UID or any national identification scheme is the question of consent and its relationship to privacy. In the case of UID project, people are totally unaware about how their information will be used and what purposes can it be used or misused for. Therefore, there is no informed consent when it comes to collection of biometric data under the UID project.

On the issue of social value it is to be noted that the value of efficiency becomes the most important value, which is valued. Many of the UIDAI documents state that the UID will provide a transactional identity. However, at the same time it takes away societal layers, which is inherently part of one's identity. In addition, it makes it possible for the identity of a person to become a commodity to be sold. This also means that the personal information has economic value and players in the market such as insurance companies, banks can buy and sell the information.

When there is identification projects using biometrics it gives the State a lot of power; the power to determine and dictate one's identity irrespective of the difference in real identity. Moreover, when such identifications projects are carried out at a national level it also gives rise to problem related to exclusion and inclusion of people or various purposes. The classification of the society based on various factors becomes easy and there is a huge risk involved with such classification.

The issues, which came out from the Q&A session, were:

- The interplay between fairness and lawfulness in the context of privacy and data collection. There has to be a question asked as to why certain information is required by the State and how is it lawful.
- In the neo-liberal era corporations are generally considered to be private. This has to be questioned and furthermore the difference between what is private and what is public. There are also concerns about corporations increasingly collaborating with the State. Can it be still considered as private?

PRIVACY AND NATIONAL SECURITY

Panelist	PK Hormis Tharakan (Former Chief of Research and Analysis Wing, Government of India), Saikat Datta (Journalist), Menaka Guruswamy, (Advocate, Supreme Court, New Delhi), Prasanth Sugathan, (Legal Counsel, Software Freedom Law Center), and Oxblood Ruffin, (Cult of the Dead Cow Security and Publishing Collective).
Moderator	Danish Sheikh (Alternative Law Forum)
Poster	Suchitra Menon (Law Student, NUJS)

Suchitra Menon discussed the legal provisions for national security in relation to privacy. Specifically, she described the guidelines and procedural safeguards with respect to phone tapping and interception of communication decisional jurisprudence.

In the year 2000, the Information Technology Act (IT Act), 2000 was enacted, this Act had under section 69 allowed the State to monitor and intercept information through intermediaries. *Prasanth Sugathan* described how the government has been trying to bypass the procedural safeguard laid down by the Supreme Court in the PUCL case by using Section 28 of the IT Act, 2000. The provision deals with certifying authority for digital signatures. The certifying authority under the Act also has the authority to investigate offences under the Act. The provision mainly deals with digital signature but it is used by the government to intercept communication without implementing the procedural safeguards laid down for such interception. Furthermore, the IT Rules which was notified by the government in April, 2007 allows the government to intercept any communication with the help of the intermediaries. The 2008 amendment to the IT Act was an after effect of the 26/11 attacks in Mumbai. The legislation has become draconian since then and privacy has been sacrificed to meet the ends of national security.

Oxblood Ruffin read out his speech and the same is reproduced below.

"The online citizenry of any country is part of its national security infrastructure. And the extent to which individual privacy rights are protected will determine whether democracy continues to succeed, or inches towards tyranny. The challenge then is to balance the legitimate needs of the state to secure its sovereignty with protecting its most valuable asset: The citizen.

It has become trite to say that 9/11 changed everything. Yet it is as true for the West as it is for the global South. 9/11 kick started the downward spiral of individual privacy rights across the entire internet. It also ushered in a false dichotomy of choice, that in choosing between security and privacy, it was privacy that had adapted to the new realities, or so we've been told.

Let's examine some of the fallacies of this argument.

The false equation which many argue is that we must give up privacy to ensure security. But no one argues the opposite. We needn't balance the costs of surveillance over privacy, because rarely banning a security measure protects privacy. Rather, protecting privacy typically means that

government surveillance must be subjected to judicial oversight and justification of the need to surveillance. In most cases privacy protection will not diminish the state's effectiveness to secure itself.

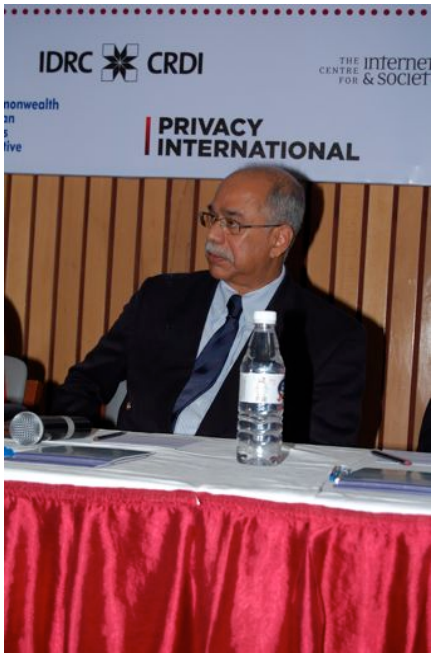
The deference argument is that security advocates insist that the courts should defer to elected officials when evaluating security measures. But when the judiciary weighs privacy against surveillance, privacy almost always loses. Unless the security measures are explored for efficacy they will win every time, especially when the word terrorism is invoked. The courts must take on a more active role to balance the interests of the state and its citizens.

For the war time argument security proponents argue that the war on terror requires greater security and less privacy. But this argument is backwards. During times of crisis the temptation is to make unnecessary sacrifices in the name of security. In the United States, for example, we saw that Japanese-American internment and the McCarthy-era witch-hunt for communists was in vain. The greatest challenge for safeguarding privacy comes during times when we are least inclined to protect it. We must be willing to be coldly rational and not emotional during such times.

We are often told that if you have nothing to hide, you have nothing to fear. This is the most pervasive argument the average person hears. But isn't privacy a little like being naked? We might not be ashamed of our bodies but we don't walk around naked. Being online isn't so different. Our virtual selves should be as covered as our real selves. It's a form of personal sovereignty. Being seen should require our consent, just as in the real world. The state has no business taking up the role of Peeping Tom.

I firmly believe that the state has a right and a duty to secure itself. And I equally believe that its citizens are entitled to those same rights. Citizens are part of the national security infrastructure. They conduct business; they share information; they are the benefactors of democratic values. Privacy rights are what, amongst others, separate us from the rule of tyrants. To protect them is to protect and preserve democracy. It is a fight worth dying for, as so many have done before us.

PK Hormis Tharakan discussed the importance of interception communication in intelligence gathering. In the western liberal democracies, restrictions of privacy were introduced for the anti-terrorism campaigns and these measures are far restrictive than what the Indian legislations contemplate. Preventive intelligence is a major component in maintenance of national security and this intelligence is generated and can be procured through interception.



We do need laws to make sure that the power of interception is not excessive or out of proportion. But the graver issue is that the equipment used for interception of communication is freely available in the market at a cheap price. This allows private citizens also to snoop into others conversation. So, interception by civilians should be the main concern.

Menaka Guruswamy discussed the lack of regulation of Indian intelligence agencies that creates burdens on privacy. When there is a conflict between individual privacy and national security, the court will always rule in favour of the national security. Public interest always takes precedence over individual interest.

When there is a claim right to privacy vis-à-vis national security, generally these claims are characterized by dissent, chilling effects on freedom of expression and government accountability. In India, privacy is fragile and relatively a less justifiable right. Another challenge to privacy is that, when communication is intercepted, which part of the conversation can be considered to be private and which part cannot be considered so.

Saikat Datta described his experience of being under illegal surveillance by an unauthorized intelligence agency. When a person is under surveillance, he or she is already considered to be suspect. If the State commits any mistake as to surveillance, carrying surveillance, who is not at all a person of interest in such case upon discovery, there is no penalty for such discrepancy.

He warned of the dangers of excessive wiretapping, a practice that currently generates such a "mountain" of information that anything with real intelligence value tends to be ignored until it is too late, as happened with the Mumbai bombings in 2008. It is clear that the Indian government's surveillance and interception programmes far exceed what is necessary for legitimate law enforcement.

The issues, which came during the Q&A session was:

- In case of national security vis-à-vis privacy in heavily militarized zone, legislations such as Armed Forces Special Powers Act actually give authority to the army to search and seizure on mere suspicion? This amounts gross violation of privacy.

PRIVACY AND BANKING

Panelist	M R Umarji, (Chief Legal Advisor, Indian Banks Associations), N A Vijayashankar, (Cyber Law Expert), and Malavika Jayaram, (Advocate, Bangalore).
Moderator	Prashant Iyengar (Associate Professor, Jindal Law University)
Poster	Malavika Chandu (Law Student, NUJS)

Prashant Iyengar highlighted how privacy has been a central feature in banking and finance. Even before the notion of privacy came into existence, banks had developed an evolved notion of secrecy and confidentiality, which was fairly robust. Every legislation dealing with banking and finance generally have a clause related to privacy and confidentiality. It might seem that it would be easy to implement privacy in banking and finance given the long relationship between banking and secrecy and confidentiality. However, this is not the case in the contemporary times. Specifically,

with the growth in issues related to national security, transparency and technology, the highly regarded notion of privacy seems to be slowly depleting.

Malavika Chandu described the data protection standards that govern the banking industry. As part of the know-you-customer guidelines, banks are required to provide the Reserve Bank with customer profiles and other identification information. Lastly, she described case laws in relation to privacy with respect to financial records.

N A Vijayashankar noted that the confidentiality and secrecy practices in the banking sector emanate from the banker-customer relationship. In the present context, secrecy and privacy maintained by the banks should be analyzed from the perspective of the right of the customer to safeguard his or her information from any third party. Generally, banks and other financial institutions protect personal information as a fraud control measure and not as duty to protect the privacy of a customer.

There has been a paradigm shift in banking practices from traditional banking practices to more efficient but less secure banking practice. Some of the terms and conditions of internet banking are illegal and do not stand the test of law. In contemporary times, banking institutions use confidentiality to cover up problems and data breach rather than protecting the customer. But the banks are not ready to disclose data breach as it apprehends that it will result in public losing faith in the system. The Reserve Bank of India, has recently notified that protection which is provided to the customers in banking services should also be extended to e-banking services. However, the banks have not properly implemented this.

M R Umarji highlighted fourteen laws related to banking which carries confidentiality clauses. In India, public sector banks dominate the market. These banks are created under a statute and such statute governs them. Therefore, they are duty bound to maintain secrecy and confidentiality. Private banks and cooperative banks are not bound by any statute. They do not have any obligations to maintain secrecy, but they do strictly observe confidentiality as a form of banking practice.

Banks are not allowed to reveal any personal information of an individual unless it is sought by some authority that has a legitimate right to claim such information. There has been a constant erosion of confidentiality due to various laws which empowers authorities to seek confidential information from the banks. Recently, in the light of the growing national security concerns, banks also have an obligation to report suspicious transactions. These have caused heavy burdens on right to privacy of an individual.

Under the Right to Information Act, 2005 public sector banks are considered to be public authorities. By the virtue of the Statute, any person can access information from banks. For example, in a recent case an information officer directed Reserve Bank of India, to disclose Inspection Reports. These reports generally contain information regarding doubtful accounts, non-performing account, etc. There is a need that banks should be exempted from the Right to Information Act, 2005. Since they are not dealing with public funds there is no need to apply transparency law to the banks.

Malavika Jayaram described the major conflicts and tensions with respect to privacy vis-à-vis banking and financial systems and financial data. Other privacy and transparency issues include: the publication of online tax information and income data.

Surveillance is built in the design of banking system, so it is capable of tracking personal information and activity. There is a need to implement more privacy friendly and privacy by design systems in the banking sector. Customers are generally ignorant about privacy policies and this influences informed consent and furthermore marketing institution may influence customers to behave in a particular manner. In this context privacy by design becomes very important.

Data minimization principles should be applied; since the more data collected the more there is a risk of data breach and misuse. In case of data retention it is necessary that person giving such data should know how much proportion of the data is being retained and for how long it is stored and also what is the scope of the data and for what purpose will it be used.

Personal information and data, which was previously collected by the government, are gradually being outsourced to private bodies. On one hand it is a good thing that private sector get their technology and security measures right as compared to the government agencies but it comes with the risk that it can be sold out by private bodies as commodities in the market. Private bodies that are harvesting the data can also be forced by the government to disclose it under a particular law or statute without taking into consideration the consent of the individual whose personal information is sought for.

There is multiplicity of documentation for identification, which makes transactions less efficient. This has attracted customers to more convenient systems such as one-access point systems, but people tend to forget the issues related to privacy, in using such a system. What is portrayed as efficient for the consumer is a tool for social control and who has access and authority to use such information.

Often the reason given for collecting information is that it will help the service provider to combat fraud. However, studies have shown people more often fake situation rather than identity. The other concerns are that of sharing of information and lack of choice with respect to such sharing. There should be check as to sharing of personal information as the data belongs to the individual

and not the bank or any other institution which requires furnishing personal information in lieu of services. This gives rise to a binary choice to the user; either the individual has to provide information to avail the service or else one cannot avail the services.

There is supposed to be market for privacy. The notion of personal information is subjective and varies from person to person. For example, one might be comfortable to share certain information. However, others might not be.

The issues that came out of the Q&A sessions are:

- The default settings are generally put at the low protection settings. Unless the user is aware of the privacy protection setting, he or she is prone to breach of privacy. Should the default privacy setting be set to maximum security and option can be given to the user to change it according to his or her preference?
- Is there any system in the banks, which allows the customers of bank to know about which all third parties the bank has shared his or her personal information with?

HEALTH PRIVACY

Panelist	K. K. Abraham, (President, Indian Network for People with HIV), Dr. B. S. Bedi, (Advisor, CDAC & Media Lab Asia), and Raman Chawla, (Senior Advocacy Officer, Lawyers Collective).
Moderator	Ashok Row Kavi (Journalist and LGBT Activist)
Poster	Danish Sheikh (Researcher, Alternative Law Forum)

Danish Sheikh outlined the possible health privacy violations. These included the disclosure of personal health information to third parties without consent, inadequate notification to a patient of a data breach, the purpose of collecting data is not specified and improper security standards, storage and disposal. The disclosure of personal health information has the potential to be embarrassing, stigmatizing or discriminatory.

Subsequently, Danish Sheikh examined the status of sexual minorities' vis-à-vis the privacy framework. Culling out some real life examples based on various studies, media reports and judgments from the Supreme Court and the High Courts of Delhi and Allahabad, he also described privacy violations committed by both individuals as well as state authorities.

Ashok Row Kavi recounted how privacy was very contextual when debating section 377 in the LGBT community. The paradigm upon which they were going to fight the anti-sodomy law was that it was consenting sex between two adults in private space. However, this paradigm was not well received by women, as women did not see private space as safe space, due to domestic violence. Perceptions of privacy are very subjective and it differs from person to person.

Raman Chawla recounted the history of the Draft HIV/AIDS Bill. In 2002, the need for law related to HIV/AIDS was realized in order to protect right to consent, right against discrimination and

right to confidentiality of HIV patients. The bill was finalized in the year 2006. Alarmingly, it is yet to be tabled before the Parliament.

The privacy provisions in the HIV bill clearly state that no person can be tested, treated or researched for HIV without the consent of the patient. It also casts that in a fiduciary relationship the health care provider must maintain confidentiality, however if the patient provides written consent then their status may be disclosed. The HIV condition of the patient can also revealed by the doctor if there is a court order demanding such disclosure. The doctor may disclose the status of the patient to his or her partner but he has to follow a particular protocol. The doctor should have sufficient belief that his or her partner is at risk of contracting HIV. The person who is infected will be asked for his/her views and counseled before his/her partner is informed. However, there are doubts as to the implementation and enforcement of this protocol.

K.K. Abraham discussed the interplay between health privacy. Health is a personal issue or experience that has public implications. The question here is whether one should be free to reveal his HIV status in public. There are two venues for treatment, the public system and private system. Treatment in private hospitals generally maintains higher standards of confidentiality. However, such treatment comes for a greater cost. On the other hand, in the public system a lot of information has to be divulged. This exemplifies discrimination in the standard of care.

Ashok Row Kavi described the process of line listing and its affect on NGO service delivery. The Government of India has introduced a method known as 'line listing'. This requires outreach workers to collect the names and addresses of every person they encounter. This list is then provided to the government. This has resulted in massive rebellion and cheating, the same people have been tested numerous times under different names. Such a mechanism has resulted in wrong and distorted statistics.

Lastly, he described the Government of India's central management information system as extremely intrusive and dangerous. This centralized database has information on approximately 300, 000 gay men, men who have sex with men, male sex workers and transgenders. Specifically, it has information on sexual activity such as if one is receptive or penetrative, number of partners, whether they have female or male partners and how many partners one has per month. He questioned the purpose of the government collecting this type of information and the ulterior motives involved for having such data.

B.S Bedi discussed the need of storage and collection standards of health data. Security and privacy standards of health data are being incorporated in health information management systems and e-health initiatives. The Ministry of Health is in the process of drafting standards for Electronic Medical Records.

CONCLUSION

Natasha Vaz (Policy Advocate, Privacy India) brought the symposium to a close by thanking the partners, the panelists, the moderators and the participants for their sincere efforts in making the All India Privacy Symposium a grand success. In India, a public discussion regarding privacy has been long over due. The symposium provided a platform for dialogue and building greater awareness around privacy issues in health, banking, national security, transparency and e-governance. Using our research, expert opinions, personal experiences, questions and comments various facets of privacy were explored.

PRESS COVERAGE

The event was featured in the media as well:

http://articles.economictimes.indiatimes.com/2012-02-02/news/31017368_1_privacy-law-privacy-international-cis

http://www.tehelka.com/story_main51.asp?filename=Ws060212Privacy.asp

http://www.dnaindia.com/analysis/column_lack-of-strong-privacy-law-in-healthcare-a-big-worry_1649366

http://www.washingtonpost.com/world/asia_pacific/privacy-concerns-grow-in-india/2012/01/26/gIQAyM0UmQ_story.html