CONFERENCE REPORT

SECURITY, GOVERNMENTS AND DATA: TECHNOLOGY AND POLICY

THE CENTRE FOR INTERNET AND SOCIETY AND THE OBSERVER RESEARCH FOUNDATION
JANUARY 8TH 2015, NEW DELHI, INDIA

Written and compiled by Lovisha Agarwaal and Nehaa Choudhari. Edited by Elonnai Hickok

CONFERENCE REPORT

SECURITY, GOVERNMENTS AND DATA; TECHNOLOGY AND POLICY

BACKGROUND TO THE CONFERENCE

The Centre for Internet and Society, in collaboration with the Observer Research Foundation, hosted a one day conference on 'Security, Governments, and Data: Technology and Policy'. The conference followed Chatham House Rules. The conference was focused on the technologies, policies, and practices around cyber security and surveillance. The conference reached out to a number of key stakeholders including civil society, industry, law enforcement, government, and academia and explored the present scenario in India to reflect on ways forward. The conference was a part of CIS's work around privacy and surveillance, supported by Privacy International.

THE CENTRE FOR INTERNET AND SOCIETY

Established in 2008, the Centre for Internet and Society is a non-profit research organization that works on policy issues relating to freedom of expression, privacy, accessibility for persons with disabilities, access to knowledge and IPR reform, openness (including open government standards, etc.) and engages in academic research on digital natives and digital humanities. CIS has offices in Bangalore and New Delhi.

THE OBSERVER RESEARCH FOUNDATION

ORF, established in 1990, is India's premier independent public policy think tank and is engaged in developing and discussing policy alternatives on a wide range of issues of national and international significance. The fundamental objective of ORF is to influence the formulation of policies for building a strong and prosperous India in a globalised world. It hosts India's largest annual cyber conference – *CyFy: the India Conference on Cyber Security and Internet Governance.*

WELCOME ADDRESS

The welcome address opened with a reference to a document circulated by CIS in 2014 which contained hypothetical scenarios of potential threats to Indian cyber security. This document highlighted the complexity of cyber security and the challenges that governments face in defending their digital borders. When talking about cyber security it is important that certain principles are upheld and security is not pursued only for the sake of security. This approach allows for security to be designed and to support other rights such as the right of

access, the right to freedom of expression, and the right to privacy. Indeed, the generation, use, and protection of communications data by the private sector and the government are a predominant theme across the globe today. This cannot be truer for India, as India hosts the third largest population on the internet in the world.

During the welcome, a brief introduction to the Centre for Internet and Society was given. It was noted that CIS is a 6.5 half year old organization that is comprised of lawyers, mathematicians, sociologists, and computer scientists and works across multiple focus areas including accessibility, internet governance, telecom, openness, and access to knowledge. CIS began researching privacy and surveillance in 2010, and has recently begun to expand their research into cyber security. The purpose of this is to understand the relationship between privacy, surveillance, and security and is the beginning of a learning process for CIS. In 2013 CIS undertook a process to attempt to evolve a legal regime to intelligently and adequately deal with privacy in India. Industry specific requirements are key in the Indian context and this process was meant to try and evolve a consensus on what a privacy law in India should look like by bringing together key stakeholders for roundtables. CIS is now in the final stages of preparing individual legal proposals that will be sent to the Government – to hopefully have an informed Privacy Law in India. This event represents CIS's first attempt to have a simultaneous dialogue on surveillance, cyber security, and privacy. As part of this event and research CIS is trying to understand the technology and market involved in surveillance and cyber security as these are important factors in the development of policy and law.

KEYNOTE ADDRESS

Presenting views as citizen of the country and not in capacity of Government Officer, the keynote speaker spoke of his experience going back to 1993 when debate and issues were beginning to emerge around the regulation of telecommunications. At that point in time, the Government of India took a view to promote and make easily accessible internet and communications technology by placing a license fee of Re. 1 for internet. Today, India is playing a big role in the internet economy- maybe in the top ten countries for internet economy.

With respect to cyber security, India started with attacks from worms and viruses. Now India deals with complex attacks from multiple sources in multiple forms on a daily basis. To make a case in point, in 2005 the Emergency Response Team responded to 250 attacks. Now in 2015, it has crossed 100,000. It is important to keep in mind that actual incidents will be greater than those reported. The rapid change in technology and type of attack makes it very difficult to do cyber security and effectively respond to all forms of cyber crime and cyber terrorism. It also creates a difficult dilemma when it comes to surveillance.

What is, though, the meaning of privacy? What is the meaning of surveillance? And what is the meaning of freedom of expression? It was noted that these questions introduce very complex subjects that do not have a clear answer.

The speaker went on to explain that India upholds and respects the right to freedom of expression and has defined reasonable restrictions to this right. India differs from the United States where the First Amendment provides absolute freedom of expression, but judgments in the US have also developed restrictions and these are similar to the ones in India. When these questions and freedoms in the context of national security and cyber security – it should be clear that there is no intention to restrict or curtail any freedom.

When it comes to cyber security, the Government has taken many steps. When looking at technology related to these areas, it should be asked if the proprietary nature of hardware/software creates regulatory problems. There is also the appreciation that judges need to be trained. Some of the judges in the High Courts of India are very active. Even the Supreme Court is very active. This is the case with the police officers also. In terms of private sector expertise in the country- Indian companies have almost the same expertise as those abroad. Indian companies are routinely involved in security audits, security solutions etc. and often help and provide support to companies abroad in these areas.

Clearly today there is a great momentum in this area- the level of appreciation and understanding is much higher. This indicates that the time has come when there needs to be open debate on what the structure and features of Internet Governance should be. On this topic, some say that there should be multi stakeholder forums; some say multi lateral. In Internet Governance- there is allocation of IP/domain name etc. but in all these aspects, the crucial part is the DNS which remains multi-lateral. This can be problematic because it is a question about operation and control of the root servers. The key note speaker concluded his speech noting again that it was his personal view.

After the keynote speech questions and comments from the audience included:

- Most of the servers that process data originating from India are located outside of India – making our emails/chats easily available to foreign powers. In this scenario, where is the privacy?
- A majority of the hardware that India has obtained is not secured; indeed the key is with someone else. We have enough laws and rules. We need strict and proper implementation.

SESSION ONE: PRESENT SCENARIO

Protecting and enhancing the cyber security of India is a complex and dynamic responsibility. The challenge of securing cyber space is magnified by the demarcated nature of the internet, the multiplicity of vulnerabilities that can be exploited at the national level, the magnitude of infrastructure damage possible from a cyber attack, and the complexity of application of a jurisdiction's law to a space that is technologically borderless. A

comprehensive 'cyber security' ecosystem is required to address such challenges – one that involves technology, skills, and capabilities – including surveillance capabilities. The Government of India has taken numerous steps to address and resolve such challenges. In July 2013, the National Cyber Security Policy was published for the purpose of creating an enabling framework for the protection of India's cyber security. In February 2014, the 52nd Standing Committee on Information Technology issued a report assessing the implementation of this policy – in which they found that a number of areas needed strengthening. The Government of India has also proposed the establishment of a number of centres focused on cyber security – such as the National Cyber Coordination Center and the National Critical Information Infrastructure Protection Centre. CERT-IN, under the Department of Electronics and Information Technology is presently the body responsible for overseeing and enforcing cyber security in India, while other bodies such as the Resource Centre for Cyber Forensic and TERM cells under the Department of Telecommunications play critical roles in overseeing and undertaking capabilities related to cyber security.

This panel explored the present scenario and the challenges that law enforcement and state security face in ensuring India's cyber security and deploying surveillance. This panel discussed threats to India's cyber security, technological and regulatory measures being taken to address such threats, challenges in implementing the same and potential future solutions.

During the panel it was discussed how there are a multitude of policies in the country which were developed when the internet was just emerging in India. Fifteen years and five months later, this same policy is still in place. What does this mean? It means government policy on encryption states that service providers cannot use more than 40-bit encryption. Yes, the Reserve Bank of India has stated that for secure mobile banking, a minimum of 128bit has to be used. The Security and Exchange Board of India says that minimum of 64bit is needed. Clearly, there is a need to have consistency between policies and current implementation in the country.

It was noted that with respect to cyber security, protected systems in India, if attacked, attract higher penalties. What is this protected system? A protected system has to be notified in an Official Gazette by the Union/State governments. To this end, it was explained that the Union Govt. has notified only one communication system (during commonwealth games- TETRA) as a protected system. States in India can also notify systems as Critical Information Infrastructure, and some states have notified all systems of the State as critical information infrastructure. It was further noted that if a system is not notified, it is very difficult to protect, and even if you notify everything as critical information infrastructure, it is still difficult to protect. To best understand how to regulate and approach critical information infrastructure, it was suggested that a cross jurisdictional analysis be completed and adopt other approaches to suit India's needs.

The boundary of what constitutes cyber space was also discussed – and it was concluded that almost everything can be brought under or connected to cyber space. For example, India is one dominant network with cable, satellite, landline, and mobile networks. The importance of understanding what is being dealt with, how different issues can be addressed, and where future trends are heading when speaking about cyber security.

Addressing relevant policy, it was highlighted that in 2011 an amendment was made to the license agreements of network operators which stated that each network operator will be responsible for the security of its networks. It was emphasized how vague this amendment is. Is there a way to define what network operators are responsible for? Are they responsible for core functions? Backhaul functions? Remote operations? In practice, this amendment has meant that everything that is connected to an operator's network is the responsibility of the operator. Even a handset is included and currently the majority of vulnerabilities coming into the network are coming from handsets. What standards applicable? In practice, any applicable standard- anywhere in the world. What is the outcome for a breach? A fifty crore penalty for every breach/every incident. There is also a five member committee to identify- penalize- blacklist- and ensure that the operator never does business in India again. Yet, there is hesitancy amongst operators to report to the government since large penalties are involved. Indeed, the Department of Telecommunications has already enforced large penalties on companies even for minor infractions.

Implementing this policy has become even more difficult as networks are now increasingly moving away from pure voice to hybrid- voice and data- now merging towards all IP based data network and security considerations are now increasing. Earlier when it was only a voice based network, security was largely limited to addressing risks on the human side. The Government of India has sought to address increasing security concerns from a policy perspective by requiring network operators to submit a certificate to the Government of India stating that their networks are secure. Yet many operators have found that when they have approached auditing firm, the firms have refused to give certificates because they are unclear as to what the applicable standards are.

Another way in which the government has tried to address security concerns is through the introduction of a certification system where every box/handset/application will be tested. As of date the government has not been able to put in place a domestic certifying lab. The government has also tried to introduce preferential market access for government departments, thus reserving a certain percentage of domestically produced technology for government procurement. Other issues with policy in India were also highlighted– including that under the Information Technology Act; intermediaries must respond to and rectify content notices within 30 days, a time period that was previously 36 hours. This is problematic as it places the intermediary in the role of an adjudicator. To help comply with this requirement operators often have a mechanism in place that at least indicates whether the notice received is genuine or not. Government regulation around online content and the challenges that governments face in balancing multiple interests and needs was also discussed. What constitutes offensive content? What constitutes acceptable content? This changes from jurisdiction to jurisdiction.

Demonstrating the sometimes present disconnect between policy makers and implementation of a policy, during the initial days of the Information Technology Act a meeting was held where eleven secretaries of the Government of India were also present. During the meeting a question was asked to the Controller of Certifying Authority about how many applications for Certifying Authority for Digital Certificate were expected to be submitted. The response was approximately 250. Participants in the meeting laughed as at the time India only had around 2,500 Internet users. Yet, overall India has not done a bad job- India was one of the first nations to put in place an Information Technology Act.

Debates by the Parliamentary Standing Committee were of quality content. Today, Indians are some of the biggest and most active users on the internet. This is something to keep in mind when we talk about law and policy. It is important to keep in mind the multiple shades of opinions in this nation. The difficulty of policy making and factoring of so many opinions will always be an issue. For example, the intent of the National Cyber Security Policy was good. The consultation with the private sector was also good. But the policy has not been implemented or operationalized.

Speaking further about cyber security, the importance of understanding when a cyber security issue adds up to a national security issue was noted. It was also noted that the defense industry has still not been drawn into the main debate around cyber security in India and it is critical for the defense forces to be intricately involved in the cyber security debate in this nation.

Questions and comments from the audience included:

- Currently, India does not have a nodal agency for cyber security. Which department should act as the nodal agency?
- What can an individual do to filter content at the household level?
- Creating certifying labs is very costly – how will this cost be met to develop the labs needed?

SESSION TWO: LAW AND POLICY

India has five statutes regulating the collection and use of data for surveillance purposes. These laws define circumstances on which the government is justified in accessing and collecting real time and stored data as well as procedural safeguards they must adhere to when doing so. The Department of Telecommunications has also issued the Unified License Agreement which, among other things, mandates service providers to provide technical support to enable such collection. The Indian judicial system has also provided a number of Rulings that set standards for the access, collection, and use of data as well as defining limitations and safeguards that must be respected in doing so. The draft Privacy Bill 2011, released by the Department of Personnel and Training, also contained provisions addressing surveillance in the context of interception and the use of electronic video recording devices.

In the Report of the Group of Experts on Privacy, the AP Shah Committee found that the legal regime for surveillance in India was not harmonized and lacked a number of safeguards. Furthermore, in the era where the direct collection of large volumes of data is easily possible, there is a growing need to re-visit questions about the legitimate and proportionate collection and use (particularly as evidence) of such data. Questions are also arising about the applicability of standards and safeguards to the state. At a global level, catalyzed by the leaks by Edward Snowden, there has been a strong push for governments to

review and structure their surveillance regimes to ensure that they are in line with international human rights standards.

This session dealt specifically with State collection of data and not private collection of data for commercial purposes and provided an overview of the law and policy applicable to data acquisition and its use in India. Ranging from discussions on the IT Act, the Telegraph Act, telecom licenses, and relevant case law– the panel looked at the present framework for data acquisition, and assessed if it has been effective, its short comings, and types of reform needed.

The panel noted that it is not possible for individuals to opt out of State data collection for surveillance purposes. Touching on the legal provisions governing the collection of data by the State, the panel discussed section 5 and subsequent 419A Rules of the Telegraph Act 1885, a 19th century legislation, which enables the interception of telephonic communications. According to the section, if there is a public emergency in existence or if the interest of public safety so warrants, then Central and State Governments and their agents can intercept or monitor any messages that passes over the telephone networks of the country.

Similarly Section 69 and subsequent Rules of the Information Technology Act 2000 makes similar provisions when it comes to collection of digital data, including content and meta data. Yet, the conditions on which this information can be collected do not include the pre-conditions of public emergency or public safety that are present in the Telegraph Act.

In addition to these provisions there are certain other provisions of law that can be used to access date. For example, section 28 and 29 of the IT Act enables the Controller of Certifying Authorities to demand user information from any of the Certifying Authorities if they think that such information is necessary in the interest of investigating contravention of the Act or any of its provision. Similarly, police officers often use section 91 of the Criminal Procedure Code to request user data such as IP addresses and stored data from service providers. In some cases the standard legal protocol that is in place for requesting such data under section 91 of the Criminal Procedure Code is not always followed.

Based on the above laws and based on such authority that is so derived from these provisions of law there is a vibrant network of lawful interception and monitoring systems in place all over India. Yet, there is not enough information in the public domain regarding what exactly are the specific systems of surveillance that the government uses to collect data. Currently, researchers in India have only been able to speculate on the frequent tenders that are floated by the government that call for private parties to supply monitoring equipment and on the product portfolios of some of the companies that have an express interest in supplying monitoring equipment. Based on this information, the kind of technology that goes into surveillance and communications in India includes things such as technology that is capable of intercepting phone calls or intercepting emails and messages and includes technology that allows for mass surveillance, big data, and mass analytic technologies.

In addition to the above there are other surveillance initiatives that have been undertaken by the government. For instance there is the Central Monitoring System, the Network Traffic Analysis software, and the National Intelligence Grid - all of which are government

developed systems. Though these are not surveillance systems as they do not collect data from the networks directly, they use the surveillance data that has already been collected by these various lawful interception and monitoring systems and they analyze this data and run certain analytics on it in order to present the data to law enforcement agencies in a way that is more useful to them.

Speaking in more detail, it was discussed on the panel how the Central Monitoring System (CMS) removes the manual chain of command that is involved in the interception process and enables law enforcement agencies to retrieve civilian data directly from the information stored in servers that are installed in the premises of telecom and internet service providers. According to statements by the government in 2013, this is a privacy enhancing measure which will ensure privacy for the citizens of India as there are lesser chances of leakage. Yet, it was pointed out that this system also removes the manual oversight of the surveillance process that exists at the moment- thus opening the system up to potential abuse by intercepting agencies.

Similarly, NETRA is an internet surveillance system which searches for keywords such as 'bomb blast' and 'kill' in India's internet traffic and allows for law enforcement agencies to access this information. NATGRID is another data collation system which collates information from 21 standalone databases. This includes databases that hold bank account details, travel itineraries, and visa details. NATGRID will collate all of these in one central database and make it available to all the law enforcement agencies.

Panelists noted that today the world is in an era where mass surveillance is possible – where technology can enable the mining and analysis of keywords, with the ability to identify and locate individuals. Currently, the government is not clear as to whether or not mass surveillance is taking place. Not discounting national security concerns, when mass surveillance is carried out it harms individual privacy. The Supreme Court of India has recognized different kinds of privacy harms, including a chilling effect on privacy that surveillance has. Theorists have also spoken about the power imbalance harm between the State and the citizens as a result of the kind of information the State has access to and is not accountable for. Currently, the National Security debate is characterized as State v. Individual right, but it is/could be viewed as a societal right v. societal right because democracy is dependent on the citizens being able to hold the State accountable. The panel highlighted the 2014 Report- Right to Privacy in the Digital Age by Navi Pillai. The Report discusses different requirements for surveillance procedures, many of which are not reflected in the surveillance procedure in place at the moment in India.

The panel also discussed how in a country like India, given the population and the size of the country, and the fact that terrorist attacks are an everyday possibility, surveillance of communications is a very powerful tool for protection of national security, yet it is also important that surveillance is not resorted to as a first resource from where data can be easily collected and used in the area of investigative processes. Thus it is critical to strike a balance between government need and user safety to ensure that principles of necessity and proportionality are in place and enforced.

During the panel a theory of what went wrong in the Indian surveillance regime was offered. It was noted that many years back when the Constituent Assembly was contemplating as to

whether the Right to Privacy should be inserted in the Constitution, this possibility was discussed in two forms. One was similar to the fourth amendment of the US style search and seizure provision and the other was a more communication- surveillance provision. Interestingly, if the Assembly debates are read, it was noted that search and seizure provisions are in the Criminal Procedure Code. A question was raised as to whether, because of the presence of search and seizure provisions, there is a need to insert such provisions in the Constitution. It was further noted that there should be search and seizure provisions in the constitution as it would create more powerful safeguards around these capabilities. Yet, the proposal was dropped over a procedural constraint and the search and seizure protections were never included in the constitution. The implications of this was that when the question of privacy safeguards came up at the time before the Supreme Court, the Supreme Court was unwilling to intervene because the Constitution makers did not insert such a right into the Constitution.

Yet, the development of case law on this subject by the Supreme Court has showed that over the years the Court has changed its mind and has started to introduce this protection in different forms. For example, the Court has recognized that surveillance does affect other rights and has a chilling effect. In the PUCL case the Court developed interim safeguards which were taken by the executive and made into the privacy safeguards for surveillance as they stand today.

When discussing surveillance, a distinction that was made by members of the panel was the difference between targeted surveillance and mass surveillance. Presently the safeguards that are in place in India address targeted surveillance i.e. when a State chooses a particular person or a particular institution to surveil on the grounds as laid out in law. In the context of targeted surveillance, it is possible to ask for a particular kind of justification i.e. why does the government want to survey this person, why is the government suspicious of this person, is this measure necessary and proportionate.

Mass surveillance is different. Mass surveillance operates in a context in which there is bulk access to communication content and related information and the government has the ability to mine the communication data for particular keywords or particular kinds of information and then identify their target. The trouble with mass surveillance is that because the specific individual is not identified and a large number of people are subject to surveillance, it is really difficult to say exactly what kind of harm results from the surveillance.

Another problem with mass surveillance is that it is difficult to develop concrete mechanisms that would offer reasonable safeguards in this particular context. This creates a situation where what is not acceptable is clear, but what is acceptable is not.

The role of private companies in state surveillance was also discussed. Highlighting the extent to which the government relies on private companies for access to stored data and content data it was noted that according to the Google transparency report from the first half of 2014 Government demands for user information have risen over 150% over the last 5 years and India is the fourth highest government that is issuing requests for user data. These numbers highlight the importance of transparency and the need for greater transparency regarding how governments are using the laws at their disposal to access user

data. From a public policy perspective, it was noted that it is important that companies create strong and transparent policies for addressing user data and surveillance requests.

Q&A Session

Questions and comments from the audience included:

- What does the panel think the obstacles in India are to reforming the law to account for warrant based surveillance?
- What is the legislative instrument through which we can seek to ensure oversight, due process principles in general on mass surveillance as well as targeted surveillance?
- The nature of surveillance now is quite different from telephone tapping in PUCL-Warrant based surveillance. A lot of the discourse about surveillance reform is shaped by PUCL which declined to create ex ante warrant requirement for surveillance. What are the challenges that the panel foresees with the course of action where the law might try to introduce this system?
- What are possible and implementable mechanisms for more transparency?
- How can accountability and oversight be built into systems of mass surveillance?
- Is it okay to do mass surveillance? Does there need to be a law that addresses this in our country.

SESSION THREE: ARCHITECTURE AND TECHNOLOGY

India is in the process of architecting a number of initiatives that seek to enable the collection and sharing of intelligence such as the CMS, NATGRID, and NETRA. At a regional level, the Ministry of Home Affairs is in the process of implementing 'Mega Policing Cities' which include the instalment of CCTV's and centralized access to crime related information. Globally, law enforcement and governments are beginning to take advantage of the possibilities created by 'Big Data' and 'open source' policing. The architecture and technology behind any surveillance and cyber security initiative are key to its success. Intelligently and appropriately designed projects and technology can also minimize the possibility of intrusions into the private lives of citizens. Strong access controls, decentralized architecture, and targeted intrusions are all principles that can be incorporated into the architecture and technology behind a project or initiative. At the same time, the technology or process around a project can serve as the 'weakest link' – as it is vulnerable to attacks and tampering. Such possibilities raise concerns about the use of foreign technology and dependencies on foreign governments and companies.

This session explored the frameworks, architecture, and technology behind such projects, explained key surveillance technologies and capabilities, and discussed if there were general principles for architecting surveillance systems that should be kept in mind.

The panel began by discussing the different legal configurations that surveillance regulation can take – noting that there are the necessary and proportionate principles, which are a set of principles that international global society organisations have agreed upon as aspects that are required for surveillance whether of data or metadata. However, it was noted that with technology such precise requirements – like a judicial warrant, are not possible to achieve. Indeed, a surveillance system that is in place and is meant for targeted surveillance can easily be put to use for indiscriminate mass surveillance as well.

It was also discussed that a lesson that India learned post 26/11 was the need to have an infrastructure that would allow agencies to share information, collaborate with each other, undertake analytics, exchange information and have a visualization layer that could really apprehend the next possible terrorist. This meant that India needed to have systems that would be able to manage data that was coming out at very high volumes, at very high velocity, at large variety, unstructured, structured, semi-structured data, and have systems that would be able to predict and undertake pattern analytics to effectively stop the next terrorist.

Today, 6 years down the line after 26/11 where is India? There are desperate systems the CMSs, the NETRA's, the FIUs in the financial side and so on. Are these systems sufficient to prevent a large scale attack nationally? There has been a paradigm change in which data is being dealt with from a need to know to a need to share basis. Is India as a nation ready to do prediction and preventive analytics? To this end, does India need a master database - like in the olden days when there was a telephone directory that would allow a person to search for somebody with just an alphabet or a name or an address? Is there a need today to have a database that would help cleanse and create a unique set of citizens of this country? India has the NPRs, the UIDs, the Election Commissions, indeed there are a plethora of organisations that have data, sensitive data to a large extent, but do these organizations need to undertake an exercise to cleanse and standardize the data they hold, and come out of a clean record of data?

When speaking about undertaking predictions it was noted that in reality law enforcement agencies receive a field report from their local representatives that they must start their investigation with. Eventually they move up the investigation life cycle, seeking transactional data from the Telco etc, and then finally reaching the stage of interception, apprehension, and arrest. This method works if law enforcement know the suspect. But when law enforcement is dealing with terabytes of data, it is much more difficult. For example, supposedly Airtel generates 50 terabytes in New Delhi alone on their data network, daily. If law enforcement have to deal with that volume of transactional data, and an equivalent volume lying with the financial institutions as well, and with the fact that this data is largely unstructured and coming in all forms and shapes and sizes, how can law enforcement undertake transactional analytics to effectively stop an attack?

There are a few systems that have been architected to address these challenges. One of these is having a trusted mediator. If law enforcement wants to look for a certain individual who is making a call from the border between India and Nepal in UP, law enforcement clearly cannot go on a phishing expedition with Airtel. But how then does law enforcement check for such an individual before harm is done? Clearly there is a need for architectures

that will allow us to test out these hypotheses on anonymized smaller datasets given the context of the rules that within which the providing organisations work, use their policies, translate them to rules, give them context, give them hierarchies, accesses, preferences, the entire spectrum of controls that will ensure that they trust the mediator to provide that data. Clearly, there is a huge challenge here in how this can be done and what is needed is a resolved dataset and access to data, otherwise law enforcement is left to look for needles in haystacks of needles.

The risks of building surveillance capabilities and architecting systems for surveillance without taking privacy seriously were also discussed on the panel. To highlight this point, the architecture of NETRA was discussed. It was pointed out that a flaw in NETRA is that it cannot examine more than 700mb of data at any given point. So, as a result if law enforcement are trying to monitor data and can only process 700mb before the system starts crashing, everybody will then begin to try to slice the data that is wanted within that 700mb of data. This demonstrates how important it is to know about the efficacy of surveillance systems, yet there has never been such an audit on the systems that are being developed. Ultimately this raises questions about the relationship between the citizen and the State. If the State says that such measures are necessary to keep the citizenry safe, but provides no further information about the process or the effectiveness of such systems, is this really transparent enough to fully justify the measures? Moreover, in addition to not releasing information about surveillance practices, the State often removes surveillance systems out of the public domain. For example, NATGRID was removed from the purview of the RTI Act.

On a point about technology, it was noted that many mobile network operators in India do not use encryption system on the radio network or the GSM. This leaves all communications transmitted on the network vulnerable and with an IMSI Catcher it is possible to easily intercept the communications. This is particularly problematic when agencies and law enforcement circumvent the legal architecture that is in place to allow for surveillance. For example, in 2006 it was found that NTRO had purchased 2006 machines which can completely go around the legal architecture allowing for surveillance.

Returning to the architecture of surveillance systems it was noted that there are problems in the architecture of surveillance systems which have a bearing on the privacy. The first is the human element. When officials practice very poor cyber hygiene this can create serious problems. For example, there was a classified database in India which was not supposed to be connected to the Internet. This database had access to a large number of government databases, and had 400 servers attached to it. There were clear security instructions that this database was not supposed to be connected to the internet. A surprise check revealed that almost 80-85% of the systems were connected to the internet. This was accidental and an issue of awareness, demonstrating the need to emphasize skill building.

Another challenge lies in bureaucratic turf battles. When one government agency does not trust the other government agency and there is little cooperation, this undermines the national security of the country. This in a sense reflects what happened to India's efforts to set up the National Counter Terrorism Centre (NCTC). There was no trust between the agencies, nobody wanted to give the operational powers to NCTC and therefore it became the casualty. The other problem is the lack of parliamentary oversight. (It was suggested

that?) All the intelligence agencies in India, barring few, carry out surveillance without any legal or constitutional backing. Though there have been efforts to introduce elements of parliamentary oversight, these have been deeply resisted by the intelligence agencies.

Another point that was made during the panel was that of human intelligence. As more and more pieces of technical information are collected, the focus has been on the technical aspect with paying only a little attention to the human intelligence aspect. Indeed, it is important to have to a comprehensive picture of the information that is coming in because if there is no proper analysis or collaboration of the data it can result in an operational failure. There is the example of Mehdi Biswas, the Twitter Jihadi, even though India had a system like NETRA in place, it was only when a foreign media pointed out his location in Bengaluru, that the local intelligence agencies and the local security agencies got a wind of it and arrested him. The other example is that surveillance architectures focus on keywords – which can result in false assumptions. In one case there was an SMS sent by one friend to another friend on his birthday saying "have a blast". The system picked up the word blast and the individual became a terror suspect. It was only when it was proved that he had sent to another person the SMS on his birthday that he was released.

Crowd sourcing surveillance (explain the technique) was also discussed during the panel, and it was pointed out that this technique only creates situational awareness and there is no strategic awareness.

It was also noted on the panel that it is important to keep in mind that when talking about surveillance, the success of intelligence agencies are seldom known while their failures are highly publicized. But notwithstanding that today India is going towards more technological regimes where technology is dictating what kind of surveillance technique you are going to undertake.

The panel also discussed the importance of building systems that both effectively and accurately analyze data for law enforcement purposes, noting that India is still in the process of building systems which can do this. Referring to past incidents, it was brought out that though in some cases Indian agencies have been able to identify and respond to threats, in other instances, due to issues regarding data collection, analysis, and sharing – they have not. It was stressed that Indian systems need to be designed to allow for proactive actions by law enforcement and agencies – while maintaining and respecting individual privacy. Other panellists highlighted the importance of proportionate, lawful, and necessary collection of data- noting that this has not been the practice in India and there have been past instances of unauthorized surveillance by the government. Furthermore, the need for governmental transparency and accountability was stressed. The government should be able to demonstrate to the public why a certain power is necessary and how it has been effective or ineffective.

Other panellists appreciated the importance of the topic, noting the critical role that telcos play in state surveillance and the need to ensure that telecommunication equipment used in India has been audited and security cleared. As in other panels, the dilemma that the government faces in trying to address threats while still maintaining individual privacy was brought out in the discussions.

Questions and Comments from the audience:

- Does India export surveillance technology and is there regulation over this?
- How is mass and indiscriminate collection of data useful to law enforcement and agencies? Is it really necessary, and if it is, do we need to amend Indian law to account for mass surveillance?

SESSION FOUR: INTERNATIONAL AND DOMESTIC MARKETS

Globally, the security market is growing – with companies offering a range of services and products that facilitate surveillance and can be used towards enhancing cyber security. In India, the security market is also growing with studies predicting that it will reach $1.06 billion by 2015. Recognizing the potential threat posed by imported security and telecom equipment, India also develops its own technologies through the Centre for Development of Telematics –responsible for the development of telecom equipment, and the Centre for Development of Advanced Computing – attached to the Department of Electronics and Information Technology. At times India has also imposed bans on the import of technologies believed to be compromised. Towards this end, the Government of India has a number of bodies responsible for licensing, auditing, and certifying the use of security and Telecommunication equipment. Though India has recognized the security vulnerabilities posed by these technologies, as of yet it has not formally recognized the human rights violations that are made possible. Indeed, though India has submitted a request to be a signing member of the Wassenaar agreement, they have yet to be accepted.

This session looked at the security market in India, from key actors and technologies, to the policy and regime behind this market, the session also shed light on the process of developing, importing, exporting, and selling security equipment in India.

During this session the panel discussed a number of topics including different forms of authentication for secure transactions, the privatisation of security related research by governments, and the growing global security market. The panel discussed the increasingly close relationship between private companies and governments, with companies facilitating government access to customer data or building vulnerabilities into their systems that can be exploited by governments.

It was discussed on the panel how there are a whole range of market interventions that have been proposed by governments across the world. One requirement after the Snowden's revelations has been data localization. Indeed, many governments across the world are asking for data localization. Another proposal has been the mandatory domestic routing of domestic traffic. This is another proposal that has been mentioned in the Indian context and also in the context of certain other countries. Brazil has laid a cable so that its traffic

need not and cannot be intercepted by American intelligence agencies when it travels to Europe.

The panel also discussed cyber security in the context of secure mobile banking and payments. Currently in India, when individuals provide the required Know Your Customer information to the bank - their photograph, address and signatures are stored in the same filing tray. This current system leaves such information vulnerable to attack. Though there are some basic precautions that everybody can take i.e. not using public wifi for banking purposes, not posting personal information to social media, there is still a high risk of an attack. What is really required to any kind of cyber security is a change of method of identification.

The panel also discussed how there are whole range of proposals which nation States are considering hoping that those proposals will result in stronger cyber security. Some of these proposals contradict the architectural principles of the Internet. For e.g. the proposal mandatory domestic routing of domestic traffic, if it is done by tampering with routing tables, which interferes with the default architecture of the Internet, if it is done by increasing the size of the pipes having much more fiber optic within the country then that is a legitimate from the internet design perspective to implement the very same proposal.

Another proposal from Gaurav Raj Upadhyay who works in Nepal was discussed. The proposal suggested that instead of building a separate fiber optic network for the government, every time any private party puts down a fiber optic cable you ask for a fiber pair and then you terminate that fiber pair separately and so on and so forth. Another that has been considered is preferential market access or indigenous manufacturing also referred to on previous panels as testing and audit labs and certification. In fact Huawei is the only manufacturer of telecom equipment that is willing to share source code with nation States and when the Indian Institute of Science said that they needed a technical partner in order to run the audit lab, they were the only partner who bid for that project and unfortunately because of conflict of interest IISc could not accept it. So, there are a range of options and as a technical person, many of these technical options come with market sanction. They do not exist as a technical option in a vacuum.

It was also discussed on the panel that there has to be a clear de-hyphenation between what is privacy or cyber security as per the interpretation of the State and the interpretation of the global individual. A problem with cyber security is that it is a statist narrative that is also increasingly involving the private sector and there is a huge amount of silence when it comes to corporate security vendors and their practices. Furthermore there is a growing trend to build vulnerabilities and back doors into existing products which are then leveraged by governments.

CONCLUSION

In conclusion, the conference hosted a variety of ideas, debate, and dialogue. Participants and speakers touched on a range of issues including internet governance, surveillance, regulatory frameworks, and ICT technologies. The vast variety of topics discussed highlighted how these topics and sectors are increasingly becoming interconnected, with internet governance policies having implications for surveillance practices and markets driving changes and developments in all areas. The conference also brought out that though these sectors and topics might overlap, they also contradict and conflict with each other at times. One technology that might enable surveillance also violates privacy and challenges freedom of expression while one policy reform that enhances privacy could also undermine or challenge national security.