IEEE EXPERTS IN TECHNOLOGY AND POLICY (ETAP) FORUM ON INTERNET GOVERNANCE, CYBERSECURITY AND PRIVACY

DELHI, INDIA
4 MARCH 2016

IEEE

Version: 16 June 2016

Contents

Executive Summary

"Universal Access for Social and Economic Inclusion" was the main theme of the IEEE Experts in Technology and Policy (ETAP) Forum on Internet Governance, Cybersecurity, and Privacy in Delhi, India, on 4 March 2016. This was the fourth in a series of regional meetings—"local conversations on a global scale"—to be organized by the IEEE Internet Initiative to connect technology developers and policy makers in a uniquely meaningful way. The two sub-themes of the Delhi event were "Security and Privacy Using Biometrics" and "Technologies and Policies for Last-Mile Access and Inclusion."

Government and industry representatives, legal practitioners, and academics gathered from around the world at Le Meridien Hotel in Delhi for the one-day event. Participants heard keynote presentations and panel discussions on challenges and opportunities in technology and policy. Later in the event, they shared specific technology and policy concerns in a rapid-fire session that considered the top issues identified in previous IEEE ETAP Forums and added new concerns to the list. This discussion resulted in a list of 12 key issues (see Appendix III), and participants then voted to conduct in-depth breakout conversations around three of those issues:

- Protecting Internet traffic, managing metadata analysis, and how to implement both security and privacy at scale
- Multi-stakeholder Internet governance
- Options and challenges in providing universal access for social and economic inclusion

Follow-up actions were initiated to further refine the scopes and develop white papers on the topics of protecting Internet traffic (encryption by default) and options and challenges in providing universal access.

The next regional IEEE ETAP Forum gatherings are scheduled for 17 May 2016 in Beijing, China, and 22 June 2016 in Tel Aviv, Israel.

Introduction: IEEE Internet Initiative and IEEE ETAP Forum Series

While tremendous innovation, economic growth, and societal good have already resulted from Internet proliferation globally, the benefit to humanity that is still to be realized is potentially even greater. A transformation is underway around the world in the gathering Internet of Things (IoT). With more and more Internet-enabled devices being networked with one another, the possibilities for new services, improved productivity and efficiency, real-time decision-making, and innovative user experiences are exploding.

At the same time, however, new issues are arising in cybersecurity, privacy, and Internet governance in markets around the globe as the IoT envelops more networked objects that are capable of sensing and communicating. Collaboration across traditional professional, technological, and geographic borders will be necessary to successfully address those issues and encourage sustainable development, ongoing economic growth, and public safety and security.

The IEEE Internet Initiative facilitates a two-way dialogue between the two historically disparate worlds of technology and policy. Just as ongoing Internet innovation, sustainability, and market growth are dependent on informed Internet policy, effective Internet public policy is dependent on sound, neutral technical guidance. The IEEE Internet Initiative provides a neutral environment for collaboration among engineers, scientists, industry leaders, and others engaged in an array of technology, policy, and industry domains around the world—to the collective benefit of *all* stakeholders. In this way, the initiative helps both to boost knowledge about technology and its implications and impact on Internet governance issues and to improve awareness of public policy issues and processes in the global technical community.

The IEEE ETAP Forum on Internet Governance, Cybersecurity, and Privacy provides a unique platform for this conversation. Organized by the IEEE Internet Initiative, IEEE ETAP Forums are a series of events that bring together technology developers and policy makers to discuss and debate current and future real-world issues being confronted in public policy and technology for cybersecurity, privacy, and multi-stakeholder Internet governance—issues that impact everyone on global, national, and local levels alike. The first IEEE ETAP Forum took place in May 2015 in San Jose, California, in the United States (http://sites.ieee.org/etap-sanjose/). The next IEEE ETAP Forum events took place in Tel Aviv, Israel, in August 2015 (http://sites.ieee.org/etap-israel1/) and in Washington, D.C., USA, in February 2016 (http://internetinitiative.ieee.org/events/etap/etap-forum-in-washington-dc), followed by the gathering in Delhi, India, on 4 March 2016.

As one of the co-moderators of the event in Delhi, Deepak Maheshwari, director of government affairs for Symantec across India and ASEAN region, opened the 4 March IEEE ETAP Forum by welcoming participants. He pointed out that India is home to the second-highest number of IEEE members, behind the United States. “Here, the whole idea in the event is to create a platform for discussion,” Mr. Maheshwari said. “It’s not about coming to a specific decision or a particular standard at the end of the day. Yes, it could as well be the start of a new work stream within IEEE … but the whole idea is how to have a good interaction between the policy makers and the technologists.”

Delhi IEEE ETAP Forum Invited Speakers

Following introductions and a review by James W. Wendorf, program director of the IEEE Internet Initiative, of the previous three IEEE ETAP Forum gatherings, the Delhi event opened with three keynote speakers:

- Nitin Desai, special adviser to United Nations Secretary-General for Internet Governance, India
- Shri R.S. Sharma, chair, Telecom Regulatory Authority of India (TRAI)
- Rajendra Pawar, chairman and co-founder of the NIIT Group

Keynote Speaker: Nitin Desai

Nitin Desai, special adviser to the United Nations (UN) Secretary-General for Internet Governance, India, spoke on his experience chairing the multi-stakeholder meetings that led to the convening of the Internet Governance Forum (IGF) in 2006—"how we handled the issue of Internet governance in the early stage and how it's changed in the last 10 years."

Mr. Desai said that Internet governance presented an uncommon challenge for the UN, in that, typically, the UN had addressed issues in which policy making was in the hands of governments, and people outside government sought to have a voice in influencing that process. "The case with the Internet was the other way around," he said, with entities outside government controlling protocols and the domain name system, for example, and governments seeking to be heard. So the UN took a multi-stakeholder approach to Internet governance, in order to bring governments into conversation with the individuals who had operational control over management of the Internet, policy setting, and assignment of domain names.

Establishing Ground Rules

Four sets of stakeholders were marshalled: Internet technicians, government, civil organizations involved in access and privacy, and companies primarily involved in developing the Internet backbone and software. Then, focus turned to setting ground rules that would engender a culture of trust among participants in the early IGF work.

The first rule? "No ad hominem arguments," Mr. Desai said. If one participant disagreed with a contribution from another participant, it was not permissible to cite the contributor's country, corporation, etc. in the reason for the objection. Disagreements had to be aired and worked out strictly in context of the substance of the work.

Initial distrust among the players subsided, Mr. Desai said, as they saw that "90 percent of the decisions were mainly routine things," with no political/competitive undercurrents. "That dropped the temperature down. Then we got down to the more useful discussions on privacy and security."

Another ground rule was equal footing among participants. While the tendency in UN efforts was to

privilege governments, the IGF conversations regarded governments, non-governmental organizations (NGOs), technologists, industry, etc. as equal contributors. Also, all participants were challenged to actually weigh in. “Practically every member of the working group on Internet governance contributed something prepared in writing,” Mr. Desai said. “It forced people to trust each other.”

There were gaps in culture, behavior, and speaking style to be bridged in order “to get the ponytails and the suits to work together,” Mr. Desai said, and, moving forward, after the initial IGF report and formation, there was a need to ensure churn in personnel in order to ensure that different perspectives were reflected in conversations.

In addressing security and privacy, IGF focused development on three areas:

- End-user education (“absolutely vital … unless users are conscious of risks that are involved, you’ll never get anywhere,” Mr. Desai said)

- More robust software for handling malware (“and, even still, there will be crime and misuse”)

- Policy for handling fraud that addresses where jurisdictions lie (“that forces governments to focus attention”)

He described the group’s thinking about the relationship between the probability of a cyber criminal’s being caught and magnitude of punishment. To create effective deterrent, “if the probability of being caught is very low, then the magnitude of punishment must be very high,” Mr. Desai said. Consequently, the group reasoned, because it’s so hard to detect, Internet fraud should be penalized higher than if the fraud occurred outside the Internet.

Then and Now

Mr. Desai also discussed the evolution of the Internet governance challenge over the last decade.

“The big difference I see now is that there is much more concern about cybersecurity in context of interstate conflict and terrorism,” he said. “People are now looking at cyberspace as a separate theatre of war.”

One of the implications of this development, Mr. Desai suggested, is that there likely needs to be greater cooperation between cybersecurity technicians and those professionals who are charged with managing the use of the Internet for services such as banking, power transmission, air-traffic control, telecommunications, etc. Another change over the last 10 years is that governments are “less and less concerned about what other governments are doing but more about what major providers of Internet services are doing,” he said of search engines, social media, and other applications.

“I know that many of the answers will have to come from the community of technologists,” Mr. Desai said, “but it requires a conversation between them and the policy makers and perhaps even other stakeholders.”

Keynote Speaker: Shri R.S. Sharma

Shri R.S. Sharma, who chairs the Telecom Regulatory Authority of India (TRAI), spoke on the importance of the Internet in India's national goals. "Almost all the processes are slowly moving to the online world, and online world in our context means Internet," he said. "We must leverage Internet in the delivery of governance. This is very important for us."

He discussed the Digital India program, a flagship program of the national government premised on the vision of transforming the country into a digitally empowered society and knowledge economy. He said that the program is working to encourage development in three primary areas: digital infrastructure, software and services on demand, and citizens' digital empowerment.

The program's success, Mr. Sharma said, depends largely on expanding connectivity. He said mobile companies have made important strides in terms of lowering rates to the point of broad-scale affordability, resulting in roughly 1 person in each Indian family having mobile access. "However, what we do not have is broadband connectivity," he said. Though India has 300 million people connected to the Internet, many of those connections are low speed.

"There is a huge challenge of inclusion, and our government is working to leverage all means to improve the Internet penetration in the country," he said. There is a program to expand optical fiber to local points of presence throughout India, and other technology spaces (TV white spaces, satellite, etc.) are being explored. "There is a whole bouquet of things we propose to do to improve the Internet penetration to improve the inclusion," Mr. Sharma said.

A Seat at the Table

Mr. Sharma discussed India's motivation and efforts to play a larger role in Internet governance and decision-making around issues such as cybersecurity and privacy. With cyber terrorism and cyber warfare having "acquired dimensions which are much, much larger" and the notion of "bloodless war that doesn't involve human beings, just machines" coming into the realm of possibility, national interest and action have coalesced.

He said that concerns have grown among India's leadership that the nation has typically not had enough representation in the international bodies that make decisions about the Internet's future. "We're one-seventh of humanity … we're a very important stakeholder in this game."

Mr. Sharma said, "our laws and legal processes are really not equipped for these types of cyber crime issues," making those areas prime for innovation. He also said cyber education must be improved. "People generally think, 'If I log onto this, things are safe and sound,'" Mr. Sharma said. "We need to work very hard to see people ensure that basic precautions are taken while people are in the cyber world."

'Aadhaar'

As director general and mission director of the Unique Identification Authority of India (UIDAI), Mr. Sharma oversaw implementation of an ambitious and challenging project undertaken by the

Government of India for providing its residents with unique digital identifiers.

There were two broad drivers for the "Aadhaar" program, he said. First, millions of people have no formal document (such as a birth certificate or school certification) for proving their identity. Second, he said, "in last 20 years, India has focused on delivering (social-assistance) benefits to individuals … What happens when you give benefits? There is then a desire and propensity for people to game the system by creating multiple identities." Consequently, the need to create a system to ensure that individuals "are able to get into a database only once" also informed Aadhaar's development.

Though much of India lacked connectivity at development's outset, Mr. Sharma said that creating a future-proof system that would anticipate widespread access across the national population was a point of emphasis. The identification system does not take eligibility for entitlements, citizenship, etc. into account. Rather, the underlying architecture principle is that Aadhaar performs identification only and can be plugged into other domains. "When you go to a bank, the bank does the transactions; identity is done by Unique Identification Authority of India," he said.

"And then we built in a lot of privacy principles," he said. For example, identifiers are random 12-digit numbers, providing a number space of more than 100 billion for long-term scalability, and assigning no meaning (gender, age, etc.) to any of the digits. Also, the Aadhaar system does not allow for downloading of data—only uploading. Collected information on users is kept offline at the back end; the biometric data associated with a number is not accessible by anyone, even the government.

Keynote Speaker: Rajendra Pawar

Mr. Rajendra S. Pawar spoke primarily on the National Association of Software and Services Companies (NASSCOM) Cyber Security Task Force, which was established to build India as a global hub for providing cybersecurity solutions, developing both a cybersecurity R&D plan and a skilled workforce of cybersecurity experts. The task force is studying the Indian cybersecurity ecosystem to identify issues and challenges and create an action plan to address the priority issues. In addition to his work as chair and co-founder of the NIIT Group, which has played a key role in shaping the growth of the Indian information technology (IT) sector, Mr. Pawar is chairing the NASSCOM Cyber Security Task Force.

"We have done fairly deep and wide discussions around the country," Mr. Pawar said, seeking to answer, "What are the big issues we should look at?" The NASSCOM task force has organized their gleanings into four areas for needed development:

- *Industry*—"How do we build an industry which is serving a real need?" Mr. Pawar said. "Industry will survive only if it's serving a real need." He said India hopes to increase its share of the global cybersecurity industry from 1 percent today to 10 percent in 2025. He said such growth projects to a $35 billion industry for India, yielding creation of about 1,000 startups and 1 million jobs. Job growth, he said, is the nation's biggest priority.

- *Technology*—Mr. Pawar noted how IEEE activities are contributing to technology innovations

that are needed in India, and he emphasized "the role of academia working closely with industry to create new industry in lab and take it to market."

- Skills—Not only will skills development be required for the projected 1 million people serving in new cybersecurity jobs, Mr. Pawar emphasized the necessity of skills development and threat awareness among Internet users. "Cybersecurity is as weak as its weakest link, and everyone is a link," he said. "Everyone with a mobile phone creates vulnerability."

- *Policy*—Thus far, Mr. Pawar said, the NASSCOM task force has deliberately concentrated only a small percentage of its effort on policy needs for a number of reasons, including the fact that other entities are already at work in this space. Still, "policy will have strong bearing on how much of a $35 billion industry we can achieve" in cybersecurity, he said. "The efforts of the leadership of the nation to build not just policy but cyber command will have huge bearing" on India's success in cybersecurity.

Need for Education and Collaboration

Mr. Pawar said the NASSCOM task force is planning to confine its work to 10 categories of forthcoming recommendations. At the IEEE ETAP Forum, he discussed two cross-cutting themes he has seen across the development areas.

One is the need for more education and awareness. "In this country, we did build a capacity to create talent for the IT sector … so, there is confidence we can do that in this space, too," Mr. Pawar said. He especially encouraged input from the group assembled in Delhi in the areas of education and awareness needs.

The other theme is the need for collaboration across traditional boundaries, in areas such as technology policy development. "We need a very intense interaction among three entities: government, not just for policymaking but also as users; academia, where technology has to be created; and industry, and we're looking at startups as a symbolic aspect," Mr. Pawar said. "These three in our country, as in many countries, are big silos. In fact, within government, there are many, many silos—in country after country."

He pointed to other national models from which India can learn. For example, Mr. Pawar noted the interrelated workings of education, the military, and industry in Israel, as well as using "public funds for private good" in the United States, such as in the example of government funding for startups.

"We are building a roadmap … that will help us very quickly put together the issues that will help us get to 35 billion," Mr. Pawar said of the NASSCOM task force.

Panel Discussion

Next, Prasanto Kumar Roy kicked off a panel discussion by noting some additional characteristics of the Internet landscape in India. "Almost every Internet subscriber is essentially using the mobile," he

said. “The wireline broadband is almost negligible … so, essentially, the problem is one of mobile data access, and mobile data access has a whole range of issues, including, of course, cost.” He went on to ask the audience to consider the questions, “How is all this inclusion going to happen? … In the net-neutral regime, what will we do for universal access?”

Mr. Roy then turned the conversation to four panelists to explore the universal-access question in context of biometrics, security, access, and privacy:

- Chaim Cohen, an IoT/cybersecurity consultant
- Dr. Neena Pahuja, DG ERNET (Education and Research Network), an autonomous society under Department of Electronics & Information Technology
- Subho Ray, president for the Internet and Mobile Association of India
- Osama Manzar, founder and director of Digital Empowerment Foundation (DEF) and chair of Manthan and mBillionth awards

Biometrics

Chaim Cohen discussed how biometric systems assume and require an intimate relationship between people and technologies that collect and record the behavioral characteristics of people—and that it is incumbent upon those who conceive, design, legislate, and deploy biometric systems to consider the ethical, cultural, social, and legal contexts of those systems. For example, Mr. Cohen asked, “Is more important our personal national security, or is more important our privacy, our sense of self respect, protecting who we are, and the identities of our loved ones?” Failing to attend to such considerations and their impacts, he said, not only potentially diminishes efficacy of systems but also could yield serious unintended consequences.

Mr. Cohen explained a 2002 hotel bombing in Israel and its role in galvanizing thinking toward creation of the Israeli Biometric Data Law, as well as the ongoing debate over the importance of the physical security of a person versus the person’s privacy. The law stipulates collection of Israeli residents’ fingerprints and facial contours, integration of that data onto Israeli digital identity cards and digital passports, and creation of a biometric government database to allow for access control, identification of individuals, and assistance in locating individuals suspected of criminal activity by law enforcement officials. The law was passed in 2010, and staged implementation commenced with a pilot in 2013. Mr. Cohen detailed some of the technologies that are being used in implementations of the Israeli Biometric Data Law.

While biometric systems can benefit security, Mr. Cohen concluded, potentially lifelong association of biometric traits with an individual, their potential use for remote detection, and their connection with identity records raise important issues. Such moral, ethical, social, cultural, and legal concerns can impact a system’s adoption, acceptance, and usage. Also, biometric recognition introduces key legal issues of remediation, authority, reliability, and privacy. These factors must be accounted for in the design, development, and deployment of biometric recognition systems, and, Mr. Cohen continued, the IEEE ETAP Forum series has a role to play in providing education in such areas.

IoT Security

Dr. Neena Pahuja with ERNET India said that, when she started using the Internet in 1993, security was not even among her considerations. And she was not alone. “I think we were all exploring the world of Internet, which was absolutely new for all of us.”

The conversation about security in the rollout of IoT is already quite advanced, Dr. Pahuja said. Already, she said, understanding exists that “none of the IoT products will work without security … The consumer won’t have comfort to use the product.” Without sufficient security, for example, IoT smart-home and e-health applications could be hacked and misused for criminal purposes. Dr. Pahuja presented a diagram of seven layers envisaged for IoT: people and process, applications, data analysis, data ingestion, global infrastructure, connectivity/edge computing, and things (devices, sensors, controllers, etc.). All seven are potentially “hack-able,” she said. “There is nothing that a hacker cannot do today.”

Still, Dr. Pahuja elaborated on her optimism in meeting the challenge to “ensure the IoT has a security layer from Day 1.” Hackers typically are exposed by their patterns of behavior, and the IoT already has an integrated layer for data analysis that can be leveraged in quickly identifying those patterns. She said she expects that, while not going so far to guarantee that any product or application is 100-percent safe, guidelines can be created that certain provisions be included in IoT products to protect against specific threats, and can help create a sufficient level of security to support ongoing IoT implementation and innovation. Dr. Pahuja also expressed hope that solutions can be created that appropriately balance security and privacy concerns.

Access

Osama Manzar challenged the audience to shift their focus on the access question from inclusion to exclusion in terms of access in India. Instead of measuring the success of connecting an increasing number of communities, schools, micro enterprises, health workers, etc., those working on these issues need to think more often about the number of those institutions that do not have broadband access in order to “know the intensity of exclusion for the people who are not connected … We are now on the verge of negative growth. Half the world remains not connected.”

He proposed emphasizing “very straightforward, simple solutions” in expanding access: wireless technology, utilization of unlicensed spectrum, encouraging single-circle (service area) telecom or circle-level Internet service providers, leveraging organizations already with inroads to unconnected markets, and expanded deployment of wireless broadband public access points. Mr. Manzar also urged promoting institutional-level connectivity in order to reach large numbers of users and to provide a means for accountability.

Subho Ray noted, “a skewed view of (always giving priority to) helping the villages ... Of those 1 billion we need to connect, 500 million are in cities and towns. So I would encourage everyone to look at urban areas … Let’s shift our focus a little bit.”

He said one of the reasons for delays in connecting the unconnected has been that, “for the longest time, we have not been solving for connectivity … we have been solving for the user and a device.”

Programs focused on, for example, supplying laptops to unconnected users.

“Users already have a device; they don’t have connectivity,” Mr. Ray said. “When you are trying to connect people, you start by asking, what do people already have? They have mobile phones … And if they have mobile phones, you have to provide broadband to that.”

Mr. Manzar added: “There is a lot of suffering that India is going through because of the lack of high-bandwidth provision. We are an oral society and community … You know how strongly we have spread the TV, because it’s audial/visual. You know how strongly we have spread the mobile; it is because it is audial. It does not require you to become literate or educated to read and write.”

Privacy

Mr. Roy, Mr. Cohen and Dr. Pahuja followed with a few additional brief comments on privacy.

Mr. Roy talked about issues with mobile fraud schemes preying on illiterate users and smart-grid applications being manipulated, for example, to identify houses that are unoccupied at a given moment.

Mr. Cohen marveled at how much more and how much more quickly search-engine and social-media providers can generate data on individual users than can state-run intelligence agencies. He noted the importance of encouraging smart technologists to use their skills for the public good, and he wondered about the potential of hiring expert hackers to help create more secure systems.

Dr. Pahuja warned against simply adding complexity to security policies, for it could discourage use of the technologies and connectivity that digital-inclusion initiatives are intended to spur on.

Discussions and Next Steps

Next, the Delhi meeting considered the top issues identified in previous IEEE ETAP Forums, as well as additional concerns, for more concentrated attention.

Participants discussed live streaming of news broadcasts and other content that today is delivered by radio and television. Implementation of 5G mobile services is likely to encourage the public to listen and watch such programming live on smartphones. While this could increase the reliability and authenticity of, for example, important news reporting, hacking of live data streaming and adding or replacing unwanted information could instantaneously spur unrest among communities, groups, countries, etc. In the present TV and radio broadcasting system, programs are channelized in a highly secure manner that is in the control of the broadcaster; any abnormal broadcast may be stopped immediately, to quell the potential of violence and destruction. Similar security for live data streaming and 5G mobile transmission will be necessary so as not to jeopardize public safety and security until protection of a hacked live streaming data channel is restored.

This discussion resulted in a list of 12 key issues (see Appendix III). Participants then voted for the three highest-priority topics for further discussion:

- Protecting Internet traffic, managing meta-data analysis, and how to implement both security and privacy at scale

- Multi-stakeholder Internet governance

- Options and challenges in providing universal access for social and economic inclusion

On the topic of protecting Internet traffic, the Internet Architecture Board has recommended that all traffic be encrypted by default. The Internet Engineering Task Force is trying to develop a standard.

Rahul Sharma and Prasad Mantri volunteered to lead development of a white paper on the policy and technology implications of protecting Internet traffic (encryption by default).

On the topic of universal access, all aspects of accessibility—as defined by W3C in WAI (Web Accessibility Initiative)—should be included. Quality and availability are most important; accessibility does not need to be free.

Universal access should be tied to the United Nations Sustainable Development Goals (SDGs). Of the 17 SDGs, nine are heavily dependent on ICT improvements.

Subimal Bhattacharjee, Prasad Mantri, Subrat Prusty, and Chaim Cohen volunteered to clarify and refine the scope of a white paper to be written on the options and challenges in providing universal access.

Due to lack of time, the topic of multi-stakeholder Internet governance was not further discussed.

Conclusion

The next regional IEEE ETAP Forum gatherings are scheduled for 17 May 2016 in Beijing, China, and 22 June 2016 in Tel Aviv, Israel.

Join the Conversation

The IEEE Internet Initiative works to inform debates and decisions in privacy, cybersecurity, and Internet governance and to help ensure trustworthy technology solutions and best practices. With technology policy challenges emerging in cybersecurity, privacy, and Internet governance around the world, the IEEE Internet Initiative connects engineers, scientists, industry leaders, and others engaged in an array of technology and industry domains globally with policy experts in a neutral environment, for the collective benefit of all stakeholders. There are many ways to engage through the IEEE Internet Initiative. Please visit http://internetinitiative.ieee.org or email internetinitiative@ieee.org for more information.

Appendix I: Program

The IEEE Experts in Technology and Policy (ETAP) Forum in Delhi, India, on 4 March 2016 was the fourth in a series of regional meetings to advance a global-scale discussion about top public-policy issues in cybersecurity, privacy, and multi-stakeholder Internet governance. Diverse stakeholders from around the world—government and industry representatives, legal practitioners, and academics—gathered for the one-day event organized by the IEEE Internet Initiative.

Location: New Delhi's Le Meridien Hotel

Moderators: Deepak Maheshwari and Prasanto K. Roy

Deepak Maheshwari

Deepak Maheshwari is director of government affairs for Symantec across India and ASEAN region. A public policy and regulatory affairs professional, he has a keen interest in the interplay of technological innovation with socio-economic development. An oft-invited speaker, author, and columnist, he has played a pivotal role in evolution and development of Internet policy and digital ecosystem as an industry spokesperson and thought leader. He served two consecutive terms as elected secretary of ISP Association of India (ISPAI) and co-founded the National Internet eXchange of India (NIXI). He is a charter member of IEEE Experts in Technology and chairs the BSA Asia-Pacific Policy Committee. An engineering graduate from Indian Institute of Technology as well as a law graduate, he has previously worked with Microsoft, MasterCard, HCL, and Sify.

Prasanto K. Roy

Prasanto K. Roy is a media and digital consultant who writes and speaks on technology, digital, and green issues. He is head of media services for Trivone Digital Services. A tech journalist for over two decades, he was president and chief editor at CyberMedia for over ten years. He writes for IANS, BBC News, Al-Jazeera India, et al., and is a tech expert on shows for NDTV, CNN-IBN, Headlines Today, and others. He is a jury member for various tech juries for NDTV, CyberMedia, Nasscom, DEF's mBillionth, and others. His South Delhi home Green One is India's first TERI GRIHA green home. Mr. Roy was a physics major at St. Stephen's, Delhi.

Start Time	End Time	Program
8:30 am	9:15 am	Registration and Networking Breakfast
9:15 am	9:30 am	Welcoming Remarks Deepak Maheshwari

Start Time	End Time	Program
9:30 am	9:45 am	Self-Introduction by Participants
9:45 am	10:15 am	Review and Reporting on First Three IEEE ETAP Meetings • IEEE ETAP San Jose 2015 • ETAP Tel Aviv 2015 • ETAP Washington 2016 James W. Wendorf James Wendorf is the Program Director of IEEE's Internet Initiative, which is dedicated to connecting the global technology and policy making communities on Internet governance, cybersecurity, and privacy, to inform debate and decisions, and to help ensure trustworthy technology solutions and best practices. Through the Initiative, IEEE strives to improve the state of knowledge about technology and its implications and impact on Internet related policy issues, and to raise awareness of public policy issues and processes in the global technical community. Previously, Jim was Director of Industry Connections in the IEEE Standards Association, where he facilitated the building of industry consensus and the incubation of new standards related activities in areas such as computer security, communications, Smart Grid, and cloud computing. Prior to that he was Vice President of Standardization at Philips Electronics, where he directed corporate strategy and participation in standards activities focused on electronic content distribution, digital home networking, digital rights management (DRM), and content protection. Prior to that he was Vice President and Sector Director of Software, Interaction and Connectivity in Philips Research, where he managed and guided the strategic direction of a corporate research sector focused on digital communications, video processing, and interactive services for consumer electronics. Jim has a B.Math in computer science from the University of Waterloo, and a Ph.D. in computer science from Carnegie Mellon University.

Start Time	End Time	Program
10:15 am	11:15am	*Keynote Presentations* Nitin Desai Shri R.S. Sharma Rajendra S. Pawer Nitin Desai is the Special Adviser to the United Nations Secretary-General for Internet Governance, India. In 1993, the then United Nations Secretary-General appointed Mr. Nitin Desai at the Under-Secretary-General level to head the newly created Department for Policy Coordination and Sustainable Development. In 1997, Secretary-General Kofi Annan appointed Mr. Desai to coordinate, and subsequently head, the consolidation of the three economic and social departments. Mr. Desai is also the convener of the Executive Committee on Economic and Social Affairs, which brings together the heads of all the UN Secretariat entities directly concerned with economic, environmental, and social issues. Before joining the United Nations, Mr. Desai was the secretary and chief economic adviser of India's Ministry of Finance, and he was the senior economic adviser for the World Commission on Environment and Development (The Brundtland Commission). From 1990 to 1993, Mr. Desai was the deputy secretary-general of the United Nations Conference on Environment and Development. Mr. R.S. Sharma became the Chair of the Telecom Regulatory Authority of India (TRAI) in August 2015. Prior to joining TRAI, Mr. R.S. Sharma worked as Secretary to the Government of India in the Department of Electronics and Information Technology. He has also worked as Chief Secretary to the State Government of Jharkhand (India). His other assignments include Director General & Mission Director of the Unique Identification Authority of India (UIDAI), where he was responsible for overall implementation of this ambitious and challenging project undertaken by the Government of India for providing unique identification (christened as “Aadhaar”) to all its residents. Mr. Sharma has held important positions both in the government of India and its state governments in the past and has been deeply involved in the administrative reforms and leveraging IT to simplify administrative processes. Mr. Sharma holds a Master’s degree in mathematics from IIT, Kanpur (India) and another Master’s in computer science from the University of California (USA). Mr. Rajendra S. Pawar is the Chair and Co-Founder of the NIIT Group, comprising NIIT Limited, a global leader in skills and talent development, and NIIT Technologies Limited, a global IT solutions organization. Under his leadership, NIIT has played a key role in shaping the growth of the Indian IT sector, by creating skilled manpower to drive its momentum. Having revolutionized the IT training industry, he is now involved in establishing an innovative model in higher education, the not-for-profit NIIT University. Mr. Pawar is a Distinguished Alumnus of IIT Delhi, Fellow of the Computer Society of India, Fellow of Institution of Electronics and Telecommunication Engineers and has been awarded an honorary doctorate from the Rahul Gandhi Tech University. Acknowledging his contribution to the IT industry in India, he has been awarded the country’s prestigious civilian honor, Padma Bhushan, by the President of India in 2011. He is on the boards of Indian Institute of Management Udaipur, Indian School of Business, Scindia School, SMVD University (J&K), and the Delhi University Court. Mr. Pawar is the Chair of the NASSCOM Cyber Security Task Force that has been set up in response to Prime Minister Narendra Modi's vision to see India emerge as a global hub of cybersecurity products and services.
11:15 am	11:30 am	Tea Break

Start Time	End Time	Program
11:30 am	12:45 pm	Panel Discussion Prasanto Kumar Roy (moderator) Subho Ray Osama Manzar Chaim Cohen Dr. Neena Pahuja Subho Ray has been President for the Internet and Mobile Association of India for over 10 years. He has 19 years of experience in advocacy, public policy, and regulatory affairs in ICT sectors including software, hardware, telecom, Internet, and mobile value-added services in India. Previously, he was Director, IT & Telecom for the Confederation of Indian Industry. Mr. Osama Manzar is the founder and director of Digital Empowerment Foundation (DEF) and chair of Manthan and mBillionth Awards. He is an entrepreneur, author, speaker, editor, columnist, and new media specialist who is spearheading the mission to overcome the information barrier between India's rural sector and the so-called developed society through DEF, the not-for-profit organization founded to accomplish the mission. Chaim Cohen is an IOT/CyberSecurity consultant. He promotes the creation of innovative, inclusive applications that address a broad range of issues in making technology available, accessible, and usable by all people whatever their abilities, age, economic situation, education, geographic location, or language. With a background in IOT & neuropsychology, Chaim focuses on integrating technology to empower people with auditory, cognitive, neurological, physical, speech, and visual challenges. As a developer evangelist, Chaim is active in helping managers, designers, developers, policy makers, and researchers to be aware and take into consideration the moral, ethical, social, cultural, security, privacy, and political aspects of emerging disruptive technologies. Dr. Neena Pahuja is DG ERNET, an autonomous society under India's Department of Electronics & Information Technology. Dr. Pahuja brings in experience from the education, healthcare, manufacturing, and service industries in the area of digitization and information security and business transformation. She is an alumnus of IITD. She has over 30 years experience and has worked in TCS, SAIL, USIT, Escorts, GECIS/ Genpact, & Max Healthcare in various technology enablement roles. As part of the Digital India initiative, ERNET is helping in the connectivity to and within education institutes, corporations, and even cities. ERNET is providing smart classroom solutions for remote education centers. Dr. Pahuja is additionally supporting creation of a national-level policy for IoT at DeitY. She is also doing R&D projects on the usage of white spaces for low cost, last-mile connectivity.
12:45 pm	1:45 p.m.	Hosted Lunch
1:45 pm	2:15 pm	Synthesize and Selection of High-Priority Areas
2:15 pm	3:15 pm	Breakout Sessions—Delve Deeper Into Highest-Priority Issues
3:15 pm	3:30 pm	Tea Break

Start Time	End Time	Program
3:30pm	4:30 pm	Report from Breakout Sessions
4:30 pm	5:30 pm	Next Steps and Wrap-Up
5:30 pm	6:30 pm	Networking Reception

Appendix II: Participants

Sunusi Abdullahi Bala, academia

Sanjay Bahl, CERT

Subimal Bhattacharjee, freelancer

Sri Chandrasekaran, IEEE staff

Lohith Chowdary Chilukuri, Amrita School of Engineering

Chaim Cohen, IoT/cybersecurity consultant

Nitin Desai, special adviser to the United Nations Secretary-General for Internet Governance, India

Haziq Jeelani, Government of Jammu and Kashmir

Amit Kumar Jha, DOT

Konstantinos Karachalios, IEEE

Moreshwar Katkar, VPCOE Baramati

Mansi Kedia, Indian Council for Research on International Economic Relations

John Kulick, Siemens

Suraj Kumar, Neeti Foundation

Deepak Maheshwari, Symantec

Reena Malhotra, DoT

Prasad Mantri, Oracle India Pvt. Ltd.

Osama Manzar, Digital Empowerment Foundation (DEF), Manthan and mBillionth Awards

Karen McCabe, IEEE Standards Association, IEEE Internet Initiative

Prakash Meena, Govt. Engg. College Ajmer

Lokesh Mehra, Symantec

Muniruddin Mohammed, IEEE India

Neena Pahuja, DG ERNET

Rajendra Pawar, NIIT Group

Reji Pillai, ISGF

Subrat Kumar Prusty, DOT

Srinivasan Ramakrishnan, consultant

Subho Ray, Internet and Mobile Association of India

Prasanto K. Roy, Trivone Digital Services

Somitra Sanadhya, IIIT Delhi

Sanjaya Saxena, Graype Systems

Rahul Sharma, DSCI

Shailendra Kumar Sharma, TEC, DoT

Shri R.S. Sharma, Telecom Regulatory Authority of India

Vatsala Shreeti, ICRIER

Karthik Siddavaram

Akhilesh Prasad Singh

Vipin Tyagi, Centre for Development of Telematics

Mahesh Uppal, Com First (India) Pvt Ltd

James Wendorf, IEEE Standards Association, IEEE Internet Initiative

Appendix III: Top 12 Issues

From the list of top issues from previous ETAP Forums, and the additional topics that participants identified during the rapid-fire brainstorming session at the Delhi Forum, 12 key issues were considered for targeted breakout discussions:

- Threats and opportunities in data analytics
- Algorithmic decision making that exacerbates existing power balances and ethical concerns
- Multi-stakeholder Internet governance
- Technology-policy development process
- Protecting Internet traffic, managing meta-data analysis, and how to implement both security and privacy at scale
- End-to-end security and privacy by design
- Fragmentation of the Internet and data localization due to local policies
- User assessment of trustworthiness of devices, enterprises, and governments
- Machine-readable privacy agreements and who enforces them
- Educating users about characteristics of information society and ethics
- Options and challenges in providing universal access for social and economic inclusion
- Personal video and public safety

Appendix IV: Combined Issues List, Delhi/Washington/Tel Aviv/San Jose IEEE ETAP Forums

Delhi

- Protecting Internet traffic, managing meta-data analysis, and how to implement both security and privacy at scale
- Multi-stakeholder Internet governance
- Options and challenges in providing universal access for social and economic inclusion

Washington

- Data localization
- Education and ethics
- End-to-end security/privacy by design
- Technology-policy development process

Tel Aviv

- User assessment of trustworthiness of devices, enterprises, and governments
- Educating users about characteristics of information society
- Machine-readable privacy agreements and who enforces them?

San Jose

- Threats and opportunities in data analytics
- Multi-stakeholder Internet governance
- Protecting Internet traffic, managing meta-data analysis, and how to implement both security and privacy at scale
- Fragmentation of the Internet due to local policies and how to avoid it
- Algorithmic decision making that exacerbates existing power balances and ethical concerns
- How to best engage IEEE as a platform for contributing to the resolution of these and related issues