IEEE Experts in Technology and Policy (ETAP) Forum on Internet Governance, Cybersecurity and Privacy

Tel Aviv, Israel, 10 August 2015

VERSION: 18 SEPTEMBER 2015

Contents

IEEE Experts in Technology and Policy (ETAP) Forum on Internet Governance, Cybersecurity, and Privacy

Executive Summary

The 10 August 2015 IEEE Experts in Technology and Policy (ETAP) Forum in Tel Aviv was the second in a series of discussions on cybersecurity, privacy and Internet governance in the context of practical solutions. Two dozen government representatives, industry representatives, legal practitioners and academics gathered, and the high-priority issues distilled from the conversation were:

- user assessment of trustworthiness of devices, enterprises and governments;
- education of users about characteristics and impact of the information society, and
- machine-readable privacy agreements.

Participants discussed preparation of a draft proposal for a machine-readable privacy standard for discussion by the IEEE Standards Association (the standards-development arm of the IEEE), the Standards Institute of Israel and the Israeli Bar Association, among other stakeholders. Participants also called for development, possibly in collaboration with the United Nations Educational, Scientific and Cultural Organization (UNESCO) and others, of educational material such as games and/or icons that would encourage ethical online behavior.

At the Tel Aviv IEEE ETAP Forum, it also was agreed to plan a subsequent forum in Be'er Sheva, Israel, in 2016. An additional 2016 meeting was proposed for Bangalore, India.

Introduction: IEEE Internet Initiative and IEEE ETAP Forum Series

For several decades, technology development, standardization and policy making lived side by side, with little interaction among one another. With the advance of the networked society, digital technology is penetrating all areas of life, and the need for mutual understanding and collaboration among the technical and policy communities has grown.

The IEEE Internet Initiative was launched as a neutral platform to connect technologists and policy makers, in order to better inform both sides on the tradeoffs inherent in various policy choices regarding technology. Using the unique convening power of IEEE, the initiative brings together engineers, scientists, industry leaders and others engaged in an array of technology and industry domains globally as they become co-creators of the advancing Internet of Things (IoT) and other areas of the integrated environment generated by the Internet. The initiative strives to explore the hiccups of jurisdictional fragmentation, vis-à-vis global networking and a global marketplace for services and ideas. In addition to connecting community participants with each other, the IEEE Internet Initiative's activities include:

- supporting and facilitating the development of open standards to address cybersecurity and privacy challenges;
- working to identify societal implications of alternative technology policy solutions;
- monitoring the technology policy landscape;
- supporting, collaborating and partnering with Internet ecosystem entities, and
- connecting stakeholders to a comprehensive framework of conferences, educational programs, standards, etc.

Under the IEEE Internet Initiative's purview, the IEEE Experts in Technology and Policy (ETAP) Forums on Internet Governance started in May 2015 with a meeting in San Jose, California, in the United States. The forums are intended to foster a bottom-up global discussion about top public-policy issues in cybersecurity, privacy and multi-stakeholder Internet governance. Based on issues prioritized in different regions where IEEE ETAP Forums take place over the coming months, the conversation is to be expanded to more participants online.

IEEE recognizes the global technology and policy organizations currently at work on parallel efforts and supports and engages in them. With this, IEEE sees an opportunity to deploy its many unique attributes to contribute to the resolution of Internet-governance issues and intends to cooperate with specialized international organizations and other stakeholders on issues of joint interest. The IEEE Internet Initiative and IEEE ETAP Forums are crucial to the success of such efforts.

Tel Aviv IEEE ETAP Forum Invited Speakers

Keynote presentations at the IEEE ETAP forum in Tel Aviv were delivered by Dr. Orna Berry, Corporate Vice President Innovation, EMC Centers of Excellence and R&D Centers, and General Manager, EMC Israel Center of Excellence, and Professor Shifra Baruchson-Arbib, Dean of the Faculty for Humanities, Bar-Ilan University Israel, and founder and former Head of the Department of Information Studies. Yaniv Giat with the Standard Institute of Israel discussed the Cyber Security Standardization Program (INCP). Also, regional issues and developments related to Internet governance, cybersecurity and privacy were addressed in a panel discussion joined by:

- Maya Adulamy with the Office of the Prime Minister of Israel,
- Nir Hirshman with Hirshman's PR/ Digital Rights Association,
- Jonathan Klinger with Jonathan Klinger Law,
- Yoram Lichtenstein with Yoram Lichtenstein Law and
- Morad Stern with Internet Society – Israel.

Keynote: Uncovering the Unknown

In her keynote presentation, "The Days of the Data—Uncovering the Unknown," Dr. Orna Berry highlighted challenges in seeing and preventing attacks against information systems. Both "anonymizing" data and more sharing of information regionally or internationally are necessary in fighting the ever-growing number of attacks. She said situation exposure and the number of attacks on critical IT systems were growing and different attackers had to be fought off. "We know that we face danger—danger in producing the data, in modifying data … danger of data falling into the wrong hands."

Attack scenarios to protect against in future cyber warfare include healthcare attacks, blackouts, satellite hijacking, finance market attack and drone hijacking. All systems now are smart systems, even for monitoring; almost anything can be targeted, whether for replicating intellectual property (IP) or getting influence over individuals, and attackers are not only individual hackers but also national governments, she said.

Automation in defense has been developed to help address the growing number of attacks. This comes at a considerable cost, however. Berry cited a January 2015 Ponemon Institute report that enterprises spend $1.3 million annually managing false-positive cyber security alerts, equating to almost 21,000 hours in wasted time.[1] The significant cost underscores the fact that computing is no longer just an information technology (IT) matter, Berry said; data and the protection for the data are business-level concerns. Also, lack of trained personnel is an issue, given that automation alone is insufficient, she said, because decisions often require human intervention.

[1] https://www.damballa.com/new-ponemon-report-reveals-high-cost-dealing-false-positive-cyber-security-alerts/

Need for Collaboration

Berry also encouraged more emphasis on collaboration. In pre-networked times, she said, everybody had their own security system for their own data that needed protection. The emergence of the Internet, industrial Internet and now the IoT, however, highlights the need for greater collaboration.

Data needs to be shared, even if anonymized, Berry said. When creating defense per type of data and per type of threat "we have to be looking to each country, how data is being exchanged, voluntarily or automatically." Data sharing is not enough, she said; instead, "we need to share what prevention of threat means."

Furthermore, new methodologies have to be developed to address deficiencies. Berry pointed to cooperation of the EMC Cyber Solution Group with companies and academics at Ben Gurion University. Work is ongoing, for example, on algorithms that automatically generate tests when performing inspections in the field of unknown threats.

Another issue that Berry said demands discussion is the contradiction between continuity (allowing for recovery of data) and security. As many attacks now are advanced persistent threats, Berry noted, "if your emphasis is continuity, this is a threat to security."

Keynote: Education for Assimilating Smart Internet Usage in Multi-Cultural Societies

Professor Shifra Baruchson-Arbib in the second keynote, "Education for Assimilating Smart Internet Usage in Multi-Cultural Societies: A Need for Policy and Actions," called for joint development of a global curriculum appropriate for different ages and the use of common icons to foster understanding of privacy, freedom of expression, credibility, politeness, security, responsibility and right and wrong in the virtual realm.

Baruchson-Arbib in her keynote focused on the lag of awareness of potential problems and ethical choices to be made in the virtual world, where for the first time everybody could enjoy full freedom of expression. She said that the educational system has not been prepared to teach how to live ethically and lawfully in the virtual environment.

Lack of basic knowledge the global netizens needs

Baruchson-Arbib presented two general types of knowledge that need to be provided beside basic skills for the proper technical use of IT: social and legal implications of Internet usage. She said that her findings show that young start-up entrepreneurs, for example, lack basic skills in selecting and weighing information from various information channels. "In research that my colleague and I conducted, we found that start-up entrepreneurs are principally using Google and avoiding the use of special professional databases." Baruchson-Arbib noted that people need to learn self-defense online and understand that they could harm themselves by revealing personal information. In addition, she said, "Not everyone knows what copyright laws are included when they are downloading movies and music and privacy violations such as distribution of personal information and pictures."

The lack of understanding about the knowledge gap is like "riding a car in a traffic jam without brakes," Baruchson-Arbib said. While a large user community worldwide is conducting Internet searches, playing online games and using smartphones, potential harmful consequences loom, she said, such as societal isolation, lack of communication and a lack of personal control.

Israeli Programs to tackle the knowledge gap

Baruchson-Arbib outlined several programs underway in Israel to tackle a two-fold task of teaching responsible use of information tools and teaching how to make responsible choices:

- The Lehava Project, funded by the Israeli Treasury Department, established free Internet-usage instruction in community centers. Technical aspects were the focus of this program.
- Baruchson-Arbib herself in 1990 founded the Department for Information Studies in Bar-Ilan University and pioneered the study of social information science. The main goal of the effort is to promote awareness of information-based decision making.
- Israel's Department of Education has approved high school matriculation exams on the subject of discovery of digital information—a program that provides broad, basic knowledge in the areas of information ethics, popular wisdom, knowledge management and social media.

According to Baruchson-Arbib, much more needs to be done in educating young pupils on how to live in an ethical virtual society. She said she favors doing so by using software, especially games. "If more people will think before they click, we will make a huge step towards a more ethical virtual society," she said.

The Cyber Security Standardization Program of SII

Yaniv Giat from the Standard Institute of Israel (SII) presented the Cyber Security Standardization Program (INCP). The objectives of the program include research and the development of national security standards. Two types of risk are addressed in the program, namely procedural risks and technical risks. Issues looked at include information application systems, encryption or access control. One major goal was to identify gaps in cybersecurity standardization, Giat said.

Panel Discussion: Privacy Concerns Vs. the Start-up Boom and Open Data

During the panel discussion at the Tel Aviv IEEE ETAP Forum, biometric and health data and the level of privacy granted emerged as the main topics of discussion. In addition, a machine-readable privacy manifest was presented.

The battle over the biometrical database

Several database projects are currently under discussion by the Israeli parliament, and Nir Hirshman (Hirshman's PR/ Digital Rights Association) talked about the draft Biometrical Data Base legislation. The government is asking for a storage of fingerprints in the planned database to help protect citizens against identity theft. While Hirshman said he is not opposed to biometric passports, he does see the storage of the biometric information alongside the personal data of each citizen as a security risk.

Hirshman stated, "Given the constant stream of leaks from big databases, corporate and state, it is just too high a risk—especially considering that a compromised password could be changed but fingerprints could not. Our security and privacy will be gone when the database is hacked."

Designing for privacy?

Jonathan Klinger (Jonathan Klinger Law) made the case for privacy by design. Instead of patching up systems after implementation, privacy should be thought about by engineers when developing technology.

"Whatever we plan, we need to think of, what do we need to store? Can we not store it? Can we allow the user to store the information on his end and not in a central database?" Klinger said. "This increases privacy because the dangers of leaks, the dangers of misusing the information are far less substantial."

Open data activities and privacy concerns

Maya Adulamy (Office of the Prime Minister) spoke about how open data and privacy concerns present contradictory goals in her work as Advisor to the Israeli Government's Chief Information Officer. Following open-data initiatives in other countries, the Israeli Government was committed to tap the value of these resources, she said. Benefits were expected both for citizens who could be provided with new services that the government could not produce by itself and for the Israeli start-up economy. By opening government data collections, she said, the Israeli government successfully worked to support the ecosystem of the Israeli start-up economy.

Currently, Adulamy said, the government is in the process of mapping its data sets, focusing on the high-value data sets in the process to allow for transparency and support the ecosystem. To embrace this strategy, fundamental changes are needed in how the administration looks at the data that it holds. Whereas governments previously operated as though these data belonged to them, most governments today see the information they hold as belonging to the public, Adulamy said.

Despite this change in ideology, major difficulties remain to releasing government-held data, with privacy being one of the reasons, Adulamy said. Israel is following the European Union model for privacy, she said. For example, data sets intended for release must be checked for how much they may reveal of individuals' data, and cross-referencing of data sets must be considered. "We are taking a gentle path in trying to release as much as possible without releasing information violating privacy," she said.

A Creative Commons model to allow for user choice

Yoram Lichtenstein (Yoram Lichtenstein Law) offered a perspective on the Creative Commons licensing concept to privacy. Creative Commons' licenses have three layers: a lawyer-readable legal code, a human-readable deed and a machine-readable code.

Lichtenstein spoke of the "Creative Commoning" of privacy policies so as to be expressed through the use of labels or icons to help inform users by making conditions more transparent. Basic icons could give the users information about what data is being collected, for how long, for what purposes and whether third parties would have access to the data. He suggested that this could help users make more informed decisions.

'Cyber-Insecurity'

Morad Stern, Business Development and Innovation Manager at the Israeli chapter of the Internet Society (ISOC-IL), spoke on the lack of awareness of security and privacy among students. "Things about privacy in cyberspace are not clear to them," he said. While students are often familiar with some aspects of cybersecurity that they find highlighted in the press or social media, and while they are usually familiar various operating systems, they typically are not aware of the vulnerabilities, how easy it is to copy websites for phishing exploits and "how important it is to really think before you act and share personal information," he said.

Stern also noted that, while the digital space had been declared a national asset by the U.S. government in 2009, for example, the Israeli web space was not seen as something to be guarded in such a way, as budget and manpower spent illustrated.

Turning to smart users, regulators or self-governance for solutions?

During the subsequent discussion, panelists further addressed the existing privacy and security threat.

Focusing on privacy, some panelists saw the loss of personal privacy not only as a problem for individuals but also potential threat to national security. "If we set up a biometric data base, it could prevent the next 9/11, but it might as well be a target for the next 9/11," Klinger said. Therefore, he said, restraint is needed, from users in sharing but also from governments in collecting and storing personally identifiable data.

Conscious choice by users – be private or sell your data

There was discussion of the needs for increased user awareness that smartphones and laptops are not private devices and that the individual set of applications on these devices allows for access to and use of data by other parties. Stern said that awareness, self-constraint and self-protection comprise practically the only reliable mechanism for protection of privacy.

Conscious of the vulnerabilities and value of their data, users might also make the choice to sell them, Adulamy said. To balance individual and economic and scientific interests in opening up the medical-record database, for example, there could be an offer for users to allow use of their data for receiving free treatment in return.

Binding corporations to respect privacy and pushing back against data hunger of governments

There was discussion of need for certain rules to be set, perhaps in the Internet-governance process, to bind corporations to respect privacy. Klinger pointed to mechanisms developed in some online communities to deal with bottom-up regulation on the Internet.

There also was discussion of governments with regard to privacy and personal security and their keenness to use big data on citizens. Transport identification cards, for example, even when used in anonymized forms, would still allow profiling an individual, it was suggested, given that crossing the information of rides from home to office would allow identification of somebody and then tracking travels based on the use of the card. To offset, as Hirshman described it, “the hunger of governments to collect private data about people and citizens.” it was suggested that the job of academics and engineers gathered at the IEEE ETAP Forums was to convey the message about restraint and highlight the cooperation of governments and big corporation in data collections.

Discussions and Results

Highlighting Privacy, Its Defense and Education

Following the format used in the first IEEE ETAP Forum in San Jose, California, in May, the Tel Aviv meeting collected questions from participants in a rapid-fire brainstorming session and distilled them into a list of high-priority issues. A total of 13 individual issues (see Appendix III) were distilled from the statements during this session. The focus quite clearly was on privacy, and there was a strong push to develop actionable items in two areas: standardization of a machine-readable privacy manifest and an educational initiative that would use "gamification" and easy-to-understand icons to support informed decisions. Three high-priority clusters of issues were finally picked for further discussion:

- educating users about characteristics of information society;
- user assessment of trustworthiness of devices, enterprises and governments, and
- machine-readable privacy agreements and who enforces them.

Educating users about characteristics of information society

User awareness of risks and choices to be made today were described as still under-developed. With regard to privacy, there are choices to move away from a platform/service in some cases, but choice often is not exercised. As actors in the digital sphere, users have to make decisions for their own "health" and for the "health" of others on the Internet. Attendees discussed how Internet education should look to public healthcare education (around anti-smoking, for example), which adds social and psychological aspects to standard teaching.

It was discussed that education about ethical standards (including respect for privacy) should be as interactive as possible to reach the young generation and that games are a good option. Icons, simple graphics and common archetypes such as traffic lights could be used in order to be understandable among users globally, regardless of society and language community. There is also a need for educational efforts toward the older generation and engineers, as they write the standard code that can allow for "healthy" choices or can just not provide these from the start.

User assessment of trustworthiness of devices, enterprises and governments

Users' assessment of trustworthiness of devices and services faces considerable difficulties. Complexity in terms of services and privacy policies is one huge barrier. Choices sometimes are not possible for various reasons (there is a dominant actor in the market; opt-out is no option because it would result in exclusion; a third party has opted in for someone, such as parents deciding to put genetic samples in a database, etc.) Regulation could have a role in creating a framework or mandating for transparency and choice, especially where market power is concentrated. Higher protection might be necessary for more sensitive data.

It was also discussed how regulation might come into play to stem concentration of power that would result from unrestrained information collection by dominant players (private or public). Used as a strategic advantage, data concentration could introduce asymmetric advantages and the ability to "game" the markets, in a similar way as in high-frequency trading.

Limits of regulation include cross-border jurisdictional problems and enforcement. It was noted that a look into the banking sector illustrates that, despite considerable regulation and some international regulation, untrustworthy banking remains an issue. It was pointed out that shifting liability for lost money to banks did result in more trust for online payment but that fines for lost data are not very high, despite the fact that, once lost, data cannot be recovered.

Standards, it was discussed, can assist users in making informed choices about what balance of privacy, security and utility they prefer for which services and in gaining more granular control. For IoT, for example, there might be a need for a safe-harbor provision that preserves/establishes quadruple trust so that IoT will be used.

Machine-readable privacy agreements and who enforces them?

It was discussed that a model standard for a machine readable privacy manifest might allow negotiations of privacy standards between user devices and applications or services. Applications could express what kind of data they would ask from the user device, what they would store, where data would be stored and for how long, with whom data would be shared and more. A user application could react by blocking certain uses or cutting a connection, depending on how the user set privacy levels. The system could be adjustable to various legal regimes.

With a technical standard in place, it was discussed, easy-to-use applications that were ready to read the manifest could help the user to understand what he or she is buying into. One could think of privacy scoring (green for maximum privacy friendly, red for "do not go there," etc.), and icons such as stop signs could be based on the system. It also could open a new market for privacy-information applications and services. It was suggested that companies might be forced to be more transparent about their data policy but, in turn, save money from litigation.

It was discussed that earlier efforts such as P3P of the W3C should be re-considered and learned from, in light of the new interest in privacy and cybersecurity.

Additional Items

Additional items that were discussed at the Tel Aviv IEEE ETAP Forum included issues such as big data environments and revolving doors, a closer look to false positives and the loss of autonomy for individuals by algorithm decisions, as well as some of the topics from the high-priority list of the San Jose meeting, like multi-stakeholder governance of the Internet, fragmentation of the Internet and algorithmic decision-making. An effort would have to be made to consider the issue security in the same way, participants said.

Linking IEEE ETAP Forums, Looking Back from Tel Aviv to San Jose

Tel Aviv is the second regional IEEE ETAP Forum since the start of the IEEE Internet Initiative. Jared Bielby, University of Alberta, Canada, gave a short overview in Tel Aviv about the results of the San Jose meeting. The full meeting report is here.

Six top-priority issues were selected by the group at the San Jose forum:

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

Developments since the San Jose IEEE ETAP Forum have been to prepare for online discussions to take place using a new online collaboration platform developed by IEEE. Volunteers to take leads for some of the six issues are Jared Bielby, co-chair of the International Center for Information Ethics, and Jessica Groopman, market analyst, Alitmeter Group, both of whom participated in the San Jose meeting. Jessica Groopman in San Jose had talked about the "four pillars of business communications" for ethical use, a topic related in some aspects (transparency of data use, user control) to the educational and privacy efforts further developed in Tel Aviv.

For all top-priority issues, Jared Bielby identified core questions agreed upon during the regional forum:

1. What are the key technology, policy and market issues that are in tension regarding this issue?
2. Who are the key stakeholders and what are their interests?
3. How consistent internationally are current governance arrangements for this issue?
4. What should IEEE be doing in this space?

It was discussed that a potential fifth point of discussion could be whether users have been forsaken in a scenario in which technology facilitates to satisfy market and government demand for data.

Conclusion and Next Steps

The Tel Aviv IEEE ETAP Forum concluded with suggestion of several next steps, including:

- proposing a draft ***machine-readable privacy standard*** to be scrutinized online; exploring collaboration opportunities among the Israeli Bar Association, the Standards Institute of Israel (SII) and the IEEE Standards Association (IEEE-SA), along with other entities who have worked on such similar issues, and contacting international digital rights groups such as the Electronic Frontier Foundation;

- developing a draft proposal for an IEEE Educational Activities Board (EAB) pilot program to create, educational games that support ***ethical online behavior*** and creating a survey to identify potential partner government agencies, associations and projects;

- considering ***certification of developers*** for privacy and security best practices and ***certification for websites and applications*** for privacy and security;

- further ***promoting IEEE ETAP*** action items within IEEE, and

- ***planning future IEEE ETAP Forums*** in Be'er Sheva, Israel, connected to the Campus of Ben-Gurion University of Negev, and one in Bangalore, India.

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 on Internet Governance, Cybersecurity and Privacy is bringing together technology developers and policy makers to debate current and future Internet governance, cybersecurity and privacy issues that impact everyone on a global, national and local scale.

The IEEE ETAP Forum was moderated by Oleg Logvinov and Clint Andrews:

Oleg Logvinov

Chair, IEEE Internet Initiative
Member, IEEE IoT Initiative Steering Committee, and Chair of Scenario Track
Chair IEEE P2413 Working Group "Standard for an Architectural Framework for the Internet of Things (IoT)"
Member, Corporate Advisory Group, IEEE-SA
Director, Special Assignments, Industrial and Power Conversion Division, STMicroelectronics

Clint Andrews

Clint Andrews is a professor in the Bloustein School of Planning and Public Policy at Rutgers University, and was previously director of the Urban Planning program. His expertise is in the substance and processes of energy and environmental planning and policy. He was educated at Brown and MIT as an engineer and planner. He is a member of the American Institute of Certified Planners, a LEED Accredited Professional, and a licensed Professional Engineer. Previous experience includes working in the private sector on energy issues, helping to launch an energy policy project at MIT, and helping to found a science policy program at Princeton. Andrews currently serves on the Board of Governors of the American Collegiate Schools of Planning, and is a past member of the Board of Directors of the Institute for Electrical and Electronics Engineers (IEEE) and the International Society for Industrial Ecology, and a winner of the IEEE's 3rd Millenium Medal. His books include Industrial Ecology and Global Change, Regulating Regional Power Systems, and Humble Analysis: The Practice of Joint Fact Finding.

Location: Azure Hall

Start Time	End Time	Tentative Program
8:30 am	9:30 am	**Network and continental breakfast**
9:30 am	10:00 am	**Introductions (Oleg Logvinov)**
10:00 am	10:30 am	**Keynote Presentations** Dr. Orna Berry: Corporate Vice President Innovation EMC Centers of Excellence and R&D Centers General Manager, EMC Israel Center of Excellence Prof. Shifra Baruchson Arbib: Dean of the Faculty for Humanities Bar-Ilan University Israel Founder and former Head of the Department of Information Studies
10:30 am	12:00 pm	**Panel Discussion** — Regional issues and developments related to Internet governance, cybersecurity and privacy (Includes 15 minute Break): Maya Adulamy (Office of the Prime Minister of Israel) Yaniv Giat (Standard Institute of Israel) Orna Heilinger (ISOC – SAFE) Nir Hirshman (Hirshman's PR/ Digital Rights Association) Jonathan Klinger (Jonathan Klinger Law) Yoram Lichtenstein (Yoram Lichtenstein Law) Morad Stern (Internet Society – Israel)
12:00 pm	12:30 pm	**Rapid fire round-up of key issues from all participants**
12:30 pm	1:15 pm	**Hosted Lunch**
1:15 pm	1:45 pm	**Review and comparison of first ETAP Forum outputs and discoveries** (San Jose, CA, 18 May 2015): sites.ieee.org/etap-sanjose
1:45 pm	2:00 pm	**Synthesize and refine selection of highest priority issues**
2:00 pm	3:30 pm	**Breakout Session** — Delve deeper into highest priority issues (Includes 15 minute Break)
3:30 pm	4:30 pm	**Report-outs** from breakout teams
4:30 pm	5:00 pm	**Next steps, action plan, and wrap up**
5:00 pm	6:30 pm	**Reception**

Appendix II: Participants

Logvinov, Oleg, Director of Special Assignments, Industrial and Power Conversion Division, STMicroelectronics; Chair, IEEE Internet Initiative; Chair, IEEE P2413™ Internet of Things (IoT) Architecture Working Group; IEEE Standards Association (IEEE-SA) Corporate Advisory Group, and IEEE ETAP Ad Hoc Committee

Abib, Erik, Bar-IIan University

Ackerman, Danny, SII, Standard Institute of Israel

Adulamy, Maya, Government ICT Authority, Office of the Prime Minister of Israel

Andrews, Clinton, Rutgers University, IEEE ETAP Forum facilitator

Aranzamendez, Melissa, Customer Relations and Operations Specialist at IEEE

Auster, Shmuel, Israel Aerospace Industries - ELTA Systems Ltd., IEEE Region 8 Section Industry Amabassador

Baruchson-Arbib, Shifra, Prof., Dean of the Faculty for Humanities at Bar-Ilan University Israel

Berry, Orna, EMC Israel Center of Excellence

Bielby, Jared, University of Alberta, International Center for Information Ethics (ICIE)

Bruckman, Leon, ECI Telecom

Ceruto, Donna, Associate Marketing Manager at IEEE

Cohen, Chaim, webintegrity

Ermert, Monika, Freelance Journalist

Freiman, Ori, Ph.D. Candidate, The Graduate Program in Science, Technology and Society, Bar-Ilan University

Giat, Yaniv, SII, Standard Institute of Israel

Gilboa, Niv, Ben-Gurion University

Gordon, Latonia, Director of Standards Policy, Microsoft.

Haimov, Amil, Cobweb-Security

Hirshman, Nir, Hirshman's PR/ Spokesman of Digital Rights Association

Humenick, Noelle, is Senior Manager, Professional Services, IEEE-SA

Klinger, Jonathan, Jonathan Klinger Law

Leshem, Amir, Professor and Head of the signal processing track at the EE department, Faculty of Engineering, Bar-Ilan University

Lichtenstein, Yoav, Yoram Lichtenstein Law

Luchetta, Patrizia, Enovos Luxemburg SA, Luxemburg Institute of Health, Member of the Board of Cosmos Pharmaceuticals

Maheshwari, Deepak, Head, Government Affairs-India Region, Symantec

McCabe, Karen, Senior Director, Technology Policy and International Affairs, IEEE-SA

Medzini, Rotem, Ph.D. Candidate Haifa Center for Law and Technology, University of Haifa

Moed, Iddo, Cyber Security Coordinator, Ministry of Foreign Affairs, Israeli

Parsons, Glenn, Ericsson

Stern, Morad, Internet Society-Israel

Tepper, Harold, Senior Program Director, IEEE

Trivedi, Yatin, Synopsys

Wennblom, Philip, Intel Corporation

Appendix III: Rapid-Fire Brainstorming

Top priorities of participants of the Tel Aviv IEEE ETAP Forum presented during the rapid-fire part of the meeting:

- **User assessment of trustworthiness of devices, enterprises and governments**

  False positives and potential discrimination based on big-data efforts were mentioned as a big issue.

  A person with a genetic profile might or might not develop a certain disease; should there be legislation to restrain discrimination, for example, by insurance companies based on big data? The question touches everybody in different roles – someone could be a citizen, an employee of a company or government official, even at the same time. At the same time, fast technology changes ask for dynamic regulation.

  Can individuals still control data, by calling on a data collector to erase data? Is there a right to ask for withdrawal of data or a right to be forgotten? Can it be implemented in an effective way? How can it be effective in a cross-border network?

- **Is privacy still an issue at all?**

  One opinion voiced was that privacy is no longer an issue, as data is shared so many times that there is no incentive for self restraint. Why should the Israeli government put a halt to its biometric database, for example, when the same data—fingerprints of travellers, including those from Israel—are already stored by U.S. border control?

  Conversely, another opinion was voiced that, while some people easily give up their privacy in the hope of security or convenience, privacy is still important and that its protection should be realized through regulation and laws.

  Also touched upon was the loss of autonomy for individuals, with decision-making being moved more and more to algorithms. Not only are companies (through credit scoring, for example) but also individuals (through search-engine auto-completion) more and more being helped by machines with decisions such as who they like as a creditor or what they are, in fact, looking for. What happens when the IoT decides for us?

  One issue put forward was the effect of knowledge transfers in big data times between public and private institutions, as individuals moved between government and industry. What are the issues and potential measures to take when a former industry person becomes a regulator and when a former official takes knowledge over to the private sector?

  Another question talked through was how to limit the impact of data leaks of "non-users" for example, through mining of contact lists.

- **Standards, Certificates, Icons for Privacy**

  Certification could be a way to build trust, not only of devices, but also of institutions. Could there be privacy certificates for private and public institutions and their services?

  How might standardizing privacy policy by standardizing an XML format allow understanding around which personal information it retains? Presented in a machine-readable format, the privacy manifest could allow a user blocking information or parts of it to be transferred. A user may be assisted by an easy-to-use application for setting one's privacy level. It was discussed, who would enforce the implementation of the machine-readable privacy policy manifest, given that standards are always recommendations?

  One recommendation was made to classify private data and differentiate various levels of sensitivity/protection. Which information can be used freely? Which requires more protection?

- **Educational efforts**

  - Use of a concept of a computer-driving license (like the European Computer Driving License) in education.
  - Use of gamification to teach ethics for the virtual world.
  - Use of icons as a globalized language on basic ethical value.

Appendix IV: List of Issues

1. Complexity in categories, multiple roles for all actors, indirect effects, technological change, departure from governor/governee relationship
2. Who owns my data?
3. Living with less privacy
4. Low priority of privacy relative to utility and security
5. User assessment of trustworthiness of devices, enterprises and governments
6. Human factor in regulation (given revolving door, etc.)
7. Assuming realistic human behavior when designing governance mechanisms
8. Educating users about characteristics of information society
9. Dissolution of human autonomy, "help" from machines
10. Machine-readable privacy agreements and who enforces them
11. Extending ISO 27018 privacy standard to IoT
12. Limiting indirect impact (on "non-users," such as through mining of contact lists, and de-anonymizing data)
13. Classifying private data to different levels of protection

Appendix V: Combined Issues List, Tel Aviv/San Jose IEEE ETAP Forums

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