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

WASHINGTON, D.C. UNITED STATES
5 FEBRUARY 2016

IEEE

Version: 14 April 2016

Contents

Executive Summary

The IEEE Experts in Technology and Policy (ETAP) Forum on Internet Governance, Cybersecurity, and Privacy in Washington, D.C., on 5 February 2016 was the third in a series of regional meetings organized by the IEEE Internet Initiative with the intent of creating a platform connecting technology developers and policy makers in a uniquely meaningful way. More than 50 diverse stakeholders from around the world—government and industry representatives, legal practitioners, and academics—gathered at The George Washington University for the one-day event.

In addition to hearing keynote presentations and panel discussions on challenges and opportunities in technology and policy, participants identified nearly 40 specific concerns during a rapid-fire session and then narrowed their focus to four of those issues for more in-depth breakout conversations about possible next steps in each:

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

The forum concluded with a challenge to continue the discussions at upcoming ETAP Forums scheduled for 4 March 2016 in Delhi, India, and 17 May 2016 in Beijing, China.

Introduction: IEEE Internet Initiative and IEEE ETAP Forum Series

Internet growth has delivered tremendous innovation, economic growth, and societal good globally. Its future benefit to humanity is even more promising as more and more Internet-enabled devices network with each other. This Internet of Things (IoT) opens exciting opportunities for new services, improved productivity and efficiency, real-time decision-making, and innovative user experiences.

But with more networked objects capable of sensing and communicating, new issues are arising in the areas of cybersecurity, privacy, and Internet governance in markets around the globe. Fluidly resolving such issues in an increasingly interconnected world of machines, services, and people is critical to supporting sustainable development, ongoing economic growth, and public safety and security. New technology policy challenges are emerging, and new approaches will be required. Collaboration across traditional professional, technological, and geographic barriers is needed to meet these challenges.

Ongoing Internet innovation, sustainability, and market growth are dependent on informed Internet policy. Equally, Internet policy depends on sound technical guidance. The IEEE Internet Initiative facilitates a dialogue between the two historically disparate worlds of technology and policy. The IEEE Internet Initiative connects the technical community to global policymaking for Internet governance, cybersecurity, and privacy in order to inform debate and decisions, to help ensure trustworthy technology solutions and best practices, and to successfully address the new technology policy challenges. The 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. The IEEE Internet Initiative helps improve the state of knowledge about technology and its implications and impact on Internet governance issues, and it raises awareness of public policy issues and processes in the global technical community.

The IEEE ETAP Forum on Internet Governance, Cybersecurity, and Privacy is an important place for the dialogue between technology and policy experts. Under the IEEE Internet Initiative's purview, the IEEE ETAP Forum series serves as a platform connecting technology developers and policy makers in a uniquely meaningful way. Beginning with the May 2015 Forum in San Jose, California, in the United States, and followed by a forum in Tel Aviv, Israel, the gatherings have invigorated the global conversation about the real-world issues being confronted in different regions in public policy and technology for cybersecurity, privacy, and multi-stakeholder Internet governance.

Washington IEEE ETAP Forum Invited Speakers

The IEEE ETAP Forum in Washington opened with a technology-oriented keynote presentation by Juan Carlos Zuniga, principal engineer at InterDigital Labs, and a policy-oriented keynote presentation from Thomas Ruoff, director of innovation for the chief technology officer with the U.S. Department of Homeland Security. Next, two panel discussions addressed regional issues and developments related to Internet governance, cybersecurity, and privacy.

The day before this IEEE ETAP Forum, the IEEE End-to-End Trust and Security for the Internet of Things Workshop was conducted. The first panelists of this IEEE ETAP Forum shared insights from that workshop:

- Mark Cather with the University of Maryland Baltimore County, who spoke on IoT policy and standards;

- Florence Hudson with Internet2, who spoke on IoT scenarios and use cases;

- Richard Bennett, an independent consultant to policy-makers, who spoke on access control and identity management in the IoT, and

- Robert Martin with MITRE and Susan Hyon Parker with Carnegie Mellon Open Learning, who spoke on IoT architectural frameworks.

The second panel discussion concentrated on privacy, security, and innovation challenges in various aspects of the IoT and presented observations from both vertical and horizontal perspectives:

- Glenn Fink with Pacific Northwest National Laboratory, who spoke on the use of IoT in precision agriculture;

- Carl Landwehr with The George Washington University, who spoke on IoT and health;

- Saifur Rahman with the Virginia Tech Advanced Research Institute, who spoke on IoT and smart cities;

- William Whyte with Security Innovation, who spoke on IoT and transportation, and

- Ekaterina Rudina with Kaspersky Lab, who spoke on common approaches in different domains.

Keynote—Technology: Designing Privacy Into Internet Protocols

In his technology-focused keynote presentation, “Designing Privacy Into Internet Protocols,” Juan Carlos Zuniga with InterDigital Labs addressed the urgency of the issues faced by the professionals gathered at the IEEE ETAP Forum. He posited that people may not be able to effectively opt out of the IoT in the future and that interconnection of devices is happening so quickly that “it’s going to be very hard to stop anything that we do wrong.” he said. “So we better do it right the first time.”

Privacy in the IoT Age

Mr. Zuniga highlighted the privacy work in three standards-development organizations (SDOs) for the Internet: IEEE, the Internet Engineering Task Force (IETF), and W3C. In the privacy work of the IEEE 802® LAN/MAN Standards Committee, IETF, and W3C, efforts have been narrowly focused on individuals, limited to what can be addressed in protocol design (vs. deployment and operation), and have assumed a strictly technical scope (without reference to market-to-market political/policy differences, particular legal frameworks, or motivation for attacks).

Among the privacy threats that Mr. Zuniga has confronted in his work are identification, correlation, secondary use, disclosure, exclusion, surveillance, stored data compromise, intrusion, and misattribution.

"Identification is one of the clear ones we've been tracking," he said. "Tracking mobile devices of by-passers is a very easy job, even if devices are not connected to any network."

Correlation—profiling a user by combining multiple personally identifiable (PI) attributes—is another increasingly significant threat with the growth of the IoT. The variety of PI attributes is exploding in the IoT with sensory and communications capabilities being added to so many new devices. What behaviors about users could be correlated (and security threats introduced) if, for example, a particular light bulb with an Internet Protocol (IP) address is turned off every time a baby goes to sleep or if a light bulb is turned on every time someone in the home takes a shower?

As a result of the new challenges introduced by IoT proliferation, Mr. Zuniga said that certain "Privacy by Design (PbD)" principles are being embraced in protocol development, such as:

- That proactive/preventive, not reactive/remedial, is the preferred approach;
- That maximum privacy must be the default settings of new technologies (so the onus is not on novice users to turn on protection);
- That privacy is embedded into design;
- That there must be full lifecycle, end-to-end protection of PI information from points of data generation to termination and each point in between, and
- That as few PI attributes should be collected as possible.

Q&A

Among the questions from the audience after Mr. Zuniga's presentation was one about whether the privacy questions being addressed in the IEEE 802, IETF, and 3WC environments were medium-specific. Mr. Zuniga confirmed that, in the same way that threats are prevalent irrespective of the medium, so is the privacy work that is underway within the SDOs.

He was also asked about the purely technical approach to addressing privacy concerns. Mr. Zuniga discussed instances in which activity was legal in some markets and illegal in others. Plus, he said, "unfortunately, right now, it's very easy to track users—you don't need huge infrastructure to do a bunch of bad things in the world." To the end of protecting as many people as possible, he said, efforts have been focused on instances where, from a privacy and security standpoint, there is no difference in technical requirements of a solution, regardless of the motivation of an attack.

Keynote—Policy: Achieving a Secure and Resilient Cyber Ecosystem: A Way Ahead

In the second, policy-oriented keynote, "Achieving a Secure and Resilient Cyber Ecosystem: A Way Ahead," Thomas Ruoff with the U.S. Department of Homeland Security said, "The bad guys are getting better, and what I think is important to understand is that the attacks are getting more sophisticated at a rate that is outpacing our ability to counter them."

"If we think we can 'man' our ways out of the problem, then we're kidding ourselves. That's a policy decision that the government has made—you're not going to get enough folks; you never will," he said. "And our ability to detect and respond is too slow, so we in the Department of Homeland Security do not believe we can detect our way out of problem. It's not going to happen. Why? Because the detection methods always lag."

Consequently, the Department of Homeland Security is working toward a secure and resilient cyber ecosystem. Mr. Ruoff walked the audience through the interrelated challenges, proposed solutions, and mechanisms enabling effective and efficient risk mitigation toward achieving such an ecosystem:

- For the challenge of disparate security tools failing to provide an integrated toolset, he said, the proposed solution is interoperability. A common data model; data and transport standards; open application programming interfaces (APIs), frameworks and control planes; and rapid integration acquisition are viewed as the mechanisms for achieving interoperability.

- For the challenge of adversaries innovating at a faster rate than defenders, he said, the proposed solution is automation. A common data model, orchestration, and shared Courses of Action (COAs) are the necessary mechanisms to achieve automation.

- For the challenge of limited automated authentication, he said, the proposed solution is trust. Security architecture, authentication infrastructure, and established partnerships are the needed mechanisms to achieve trust.

- For the challenge of security analysts having incomplete knowledge and situational awareness of their enterprise and overall ecosystem security health, he said, the proposed solution is information sharing. A common data model, information sharing, and authentication infrastructure are the necessary mechanisms.

- And for the challenge that the communications infrastructure could be attacked, the solution is assured communications, with resilient communications, priority services, and interconnected infrastructures viewed as the necessary mechanisms, he said.

Toward ‘EASE’

Mr. Ruoff said that the Department of Homeland Security envisions an “Enterprise Automated Security Environment (EASE),” information-sharing infrastructure, and “cyber weather map” as inter-related components of a secure and resilient cyber ecosystem. The Department of Homeland Security’s accomplishments to date in achieving a secure and resilient cyber ecosystem, he said, are developing a request for information (RFI) for a messaging bus, a thought leaders roundtable, workshop, COA Working Group, and a focus group on the message fabric.

“We want to understand the local state of the art … we have had thought leadership, so we called in the smart folks from all of the academic and vendor communities and asked, ‘Where do you think we should go?’” Mr. Ruoff said. “We in Department of Homeland Security do not believe that we should be telling the path or defining the path. We think we should be leading from behind, facilitating the discussion. Why? Because we are humble enough to understand that we are not as smart as other people in the community, but we are in a position where facilitation will lead to success.”

Q&A

Among the questions from the audience following Mr. Ruoff’s keynote was how standards development can be informed by the DHS needs, and he encouraged attendance at the department’s periodic community-day forums.

One attendee questioned the government’s commitment to information sharing and whether that notion demanded a culture change. Mr. Ruoff said, “The president felt exactly the same way, so about six months ago he sent out a presidential directive telling the Department of Homeland Security that they have to take automated information sharing seriously.” He said substantial investment is being placed in information-sharing systems programmatics.

Another question addressed the possibility of monitoring systems being used for malware attacks on the cyber ecosystem architecture. Mr. Ruoff acknowledged this issue of “giving the adversary the keys to the kingdom—if they get inside the orchestrator, they win”—and he said creating an approach to prohibit such an attack is the focus of development activity now.

Panel Discussion: Issues Highlighted at the 4 February 16 IEEE End-to-End Trust and Security for the Internet of Things Workshop

The day before the IEEE ETAP Forum, industry technologists gathered for a workshop on the development of an open architectural IoT framework at the invitation of IEEE, Internet2, and the National Science Foundation (NSF). Presentations were given addressing “TIPPSS" elements in relation to IoT: trust, identity, privacy, protection, security, and safety. At the IEEE ETAP Forum on 5 February, participants offered summaries of four presentation tracks from the 4 February IEEE End-to-End Trust and Security for the IoT Workshop.

Policy and Standards

Mark Cather with the University of Maryland Baltimore County reported that about 10 people participated in the policy and standards track. He said one topic of conversation was the importance of consumer trust in realizing IoT potential growth, forecasted at “50 to 200 billion devices by 2020 or 2025 depending on what research you look at.”

The IoT growth forecasts suggest a meshed web of things to be secured and maintained, including devices, Mr. Cather said, “made by anyone from hobbyists, to small companies in their basements, to huge, multinational companies.” Not only does this identify the need for flexible standards that are relevant for very different manufacturers; participants noted that this diversity renders standards education a significant challenge. Another challenge with regard to standards development for the IoT will be that the security of devices will have to be thought of in terms of their system-level context—a light bulb in a bedroom and a light bulb in a surgery room will have varying needs of encryption, authentication, privacy, security, etc.

Mr. Cather said the participants discussed the need for work in the policy and standards environments to dovetail, as well as a capability to push regulatory and standards information out to IoT developers more rapidly given the faster pace of technological change.

Scenarios and Use Cases

Florence Hudson with Internet2 discussed activities in the scenarios and use cases group, which she said involved about 30 people. Participants talked about how and where technology and policy blend and the importance of creating a commonly shared language between the two worlds and identifying individuals who can connect deeply on both sides. She said that some participants feel the gap between policy and technology is actually growing.

Ms. Hudson said participants in the scenarios and use cases group discussed the need for duty and responsibilities for TIPPSS among developers and the crucial role of engineering ethics in the expanding IoT economy. Organizations from within the vertical markets of IoT development will have critical domain-specific views into such efforts. As an example, she related questions surrounding defense in depth in relation to usage of connected insulin pumps in an eHealth, distributed-care scenario: How can it be ensured that the individual checking the data from such a pump is the right healthcare provider? How frequently is the individual’s certification checked?

“One of the challenges is that people/citizens assume somebody is worrying about this for them, and that would be us,” Ms. Hudson said. “We have to go from worrying about it and being thought leaders to being ‘do’ leaders. We really have to rise to the occasion.”

Access Control and Identity Management

Richard Bennett, a consultant, reported on the discussions of the access control and identity management group at the 4 February IEEE End-to-End Trust and Security for the IoT Workshop. Topics discussed included private biometric verification, establishing connectivity in the IoT, virtual organizations, and “IoT Security: A Nightmare in Progress.”

He said that the general sense of the group was that, while access controls and authentication are not solved problems, the mechanisms that currently exist are adequate for addressing these problems. However, Mr. Bennett said, “there is clearly a gap between available technologies and the stuff people are using.”

Persistent identifiers, the group discussed, present an issue in that they can be correlated with activities, leading to discovery of things about that user and potentially create an opportunity to break into the system. Mr. Bennett said the group affirmed the importance of standards in the space and discussed the necessity of new ways of thinking about the issues of access control and identity management that are introduced in the IoT. For example, there will be interconnected devices that do not have usernames and passwords, there will be a need to identify that the correct software is controlling a system, and there will be autonomous devices that function much like people but cannot be authenticated in the same ways as human users are.

Architectural Framework

Robert Martin with MITRE and Susan Hyon Parker with Carnegie Mellon Open Learning presented on the architectural framework breakout, in which 25 to 30 people participated.

"We need to make sure we don't fall prey to calling this end-to-end security, when really we want to talk about end-to-end security *and* safety," Mr. Martin said. "It's really not a network issue. Don't take a network-security approach to this, because it's really each element, each node, the software on those nodes … If we only come to this as the integrity of the network, we will fail gloriously. For the IoT, safety needs to be considered along with privacy, the performance issues, reliability, resilience, and, of course, the security of these systems." Ms. Hyon Parker added that this led the group to discuss the need for a more holistic, rigorous systems approach for IoT systems with integrated hardware and software rules and guidelines.

The overall professionalism of the software workforce was a point of emphasis in the discussion. While every other engineering trade has established licensing and certification landscapes, the group discussed, those are not as prevalent in the software arena. Without standardized best practices and a documented understanding of software developers' qualifications, how can system reliability, security, and safety in the event of failure or malicious activity be assured?

The group discussed their perception of a general lack of respect for how transformational IoT is likely to be in policies across industries. Effective policy definition will demand that interest groups consider a whole new set of regulatory criteria as it relates to various industry situations.

Panel Discussion: Privacy, Security, and Innovation Challenges in Different Aspects of IoT

The second panel discussion offered a perspective on the challenges being confronted in IoT implementation from four vertical markets where deployment is intensifying—healthcare, smart cities, transportation, and precision agriculture—as well as the horizontal perspective of common approaches across domains.

Healthcare

Carl Landwehr with The George Washington University noted that the issues around privacy, security, and innovation in healthcare are generally well recognized. A great deal can be learned about patients and care strategies by pooling health records, but how can that information, which is clearly private and sensitive, be effectively protected? "Speaking for the U.S. legal environment, in general that information is protected if it's in a regular medical healthcare system, but it's not protected in a commercial environment," Mr. Landwehr said. "So, policy is going to have to deal with the fact that we have a tremendous amount of innovation going on at the sensor end of things."

Healthcare in the IoT presents unique challenges. For example, genomic data storage and use presents its own complex set of issues that must be addressed, he said. Hackability of medical devices is a well-known problem. Mr. Landwehr said there are efforts to move toward a "medical-device security code," along the lines of building codes that governments adopt and give legal force. More integration will be needed across the medical industry, he said, in terms of interoperability standards, protocols, and authentication techniques in the next decades. Also, innovation in personalized medicine, such as potentially networks that interconnect with humans' biologic systems, will introduce challenges.

Smart Cities

Saifur Rahman with the Virginia Tech Advanced Research Institute discussed the promise of smart cities to address urban challenges in areas such as pollution, energy efficiency, security, parking, traffic, and transportation by utilizing advanced technologies in data gathering and communications. A complex array of smart elements undergirds smart cities—energy, transportation, healthcare, e-governance, public security, etc.—"and these all have interconnections and vulnerabilities to exploit."

Smart buildings are one of the important pieces of smart cities, he said. Virginia Tech, he said, has been particularly engaged in innovation around smart buildings, which connect a building-automation system with systems for building operations (such as heating and air conditioning, lighting, water supply, sensor network, and fire emergency) for significant efficiencies. Virginia Tech provides a living laboratory for development and refinement of its Building Energy Management Open Source Software (BEMOSS) solution that is engineered to improve sensing and control of equipment in small- and medium-sized commercial buildings. Mr. Rahman said, "We focus on plug-and-play devices, because that's where the vulnerabilities come in," and then experiment with strategies for eliminating or mitigating issues.

Transportation

William Whyte with Security Innovation discussed research and innovation in connected vehicles. He said it has been estimated that, of the roughly 6 million crashes that occur in the United States annually, 4.5 million could be eliminated with IEEE 802.11™ "Wi-Fi®"-based capabilities for monitoring and communications. He said he expects future regulatory mandates to address inclusion of such technology in automobiles that would, for example, broadcast 10 times/second a vehicle's location.

Market acceptance will be a key issue to ensure that the benefits envisioned with the safety-of-life system are actually realized. If a user turns off the technology because of privacy concerns, for example, overall crash avoidance will be much less effective because devices in all the cars potentially involved in a collision must be enabled in order for the system benefit to be realized. "If you decrease penetration rate by 1 percent, you decrease the effectiveness by 2 percent when you're up near full deployment," Mr. Whyte said. "So, making this a system that people are comfortable having in their cars is vital to the overall system success."

Mr. Whyte discussed lessons learned from recent hacks of connected vehicles and issues with the remediation steps that manufacturers took. He also talked about supporting legacy technologies in connected vehicles, given that people often keep and operate individual automobiles for many years.

Precision Agriculture

Glenn Fink with Pacific Northwest National Laboratory discussed security and privacy in "the Internet of cows—and the broader area of precision agriculture," which he argued might be the oldest IoT application.

"Our interest in cows is actually as a stand-in for humans," he said. "You can really instrument cows. They are moving, living creatures, and they react to technology." Leveraging continuous monitoring for individualized care and tracking, early disease warning, farm-to-fork provenance, etc. Precision agriculture is a valuable use case with regard to the greater IoT because, he said, "we can learn a lot from cows in ways that you don't have to worry about privacy issues with humans—the cows don't worry so much about privacy."

IoT capabilities in precision agriculture effectively make visible things that were not visible before. For example, feeding can be monitored per animal. Early detection of infections by leveraging vocalization tracking and analytics can help stop disease spread. Death rates can be monitored per farm to identify problem facilities. In such ways, precision agriculture advances animal welfare and production, Dr. Fink said. Furthermore, better understanding of how animals live and work also offers important insights into how the IoT might be used to benefit humanity as well.

Common Approaches in Different Domains

Ekaterina Rudina with Kaspersky Lab discussed the general lack of readiness for IoT proliferation. "The environment is still dangerous," she said. "… Actually Internet of Things is not ready to Internet, and cyber-security is not ready to get cyber."

She described a recent "capture-the-flag" competition, in which participants from various specializations were challenged to break into a scale model of an electrical substation. Within only a few hours, third-party specialists seized control over the model substation's processes and created a total blackout. When they were interviewed after their competition the winners said the security functionality in the model was circa late 1990s.

Ms. Rudina described the promise of a "new-found second wind" of established technologies:. "Actually, we do not have to invent some new principles or new architectures," she said. "We have a lot of architectural solutions proposed many years ago, and now we can use them for contemporary technologies. Well-known security principles and practices may be applied … We have now a lot of achievements in computer security theory and a lot of achievements in the technology areas, and we just need to join these achievements to provide us with a more secure and reliable Internet of Things that is coming."

Discussions and Next Steps

Jared Bielby of the International Center for Information Ethics reviewed the previous IEEE ETAP Forum events (18 May 2015 in San Jose, California, USA, http://sites.ieee.org/etap-sanjose/forum-report/, and 10 August 2015 in Tel Aviv, Israel, http://sites.ieee.org/etap-israel1/report/). Next, the Washington meeting distilled the individual issues that participants voiced in a rapid-fire brainstorming session (see Appendix III) into a list of 10 clusters of issues (see Appendix IV). IEEE ETAP Forum co-moderator Clint Andrews with Rutgers University led participants in voting on the 10 issues and discerning four high-priority areas of concern for further discussion:

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

The results of the discussions in the breakout session are presented below.

Technology-Policy Development Process

Mary Lynne Nielsen with IEEE presented the conversation around technology-policy development process. She said the group discussed a number of levers impacting the policy landscape today, including operational best practices, guidelines, and interoperability standards; educational tools for both lawmakers and regulators; and the calls to actions flowing out of contributions from informed individuals and organizations. The group then outlined a variety of potential next possible actions:

- Progressively maturing the global-scale discussions by identifying nuggets of conversation, exploring those areas, and building communities around them;

- Creating tips and tools and/or hosting events to alleviate tension across technological and regulatory communities of different jurisdictions;

- Identifying fundamental policy principles that are being called into question by the proliferation of the IoT (for example, is the right to consent—to “opt in” or “opt out”—even feasible in the increasingly connected world?);

- Facilitating national, as well as international, conversations to address contextualized standards needs, and

- Reviewing existing standards for gaps and IoT needs.

End-to-end Security/Privacy By Design

Alan Chachich with the U.S. Department of Transportation recapped the discussion on end-to-end security and privacy by design. Agreeing that profit, cost, and features like convenience currently are higher priorities in Internet development than security and privacy protection, the group considered the question of what can be done to change incentives. Without changing that balance, there will not be a secure IoT, Mr. Chachich said, and an insecure IoT may have grave consequences for humanity.

The group created a multi-dimensional framework picture to visualize the problem being confronted and talked about how IEEE can influence progress--where are the "hot spots" where IEEE can make a difference to increase security and privacy? Mr. Chachich said that the group determined that there are two areas where IEEE might exercise influence: design and policy. He said the group looked at places where the IEEE technology activities and lobbying capacity might overlap—for example, the potential role of financial and criminal penalties around data ownership policy. He said the group agreed that, instead of imposing laws, economic incentives are probably better for all stakeholders and ultimately more useful in achieving desired results.

As for next steps, Mr. Chachich said the group suggested that IEEE could strive to create a layered model, such as the Open Systems Interconnection (OSI) network model, to guide policy. After surfacing all the important design and policy factors that could advance end-to-end security and privacy by design, IEEE could then identify those where it could have the most impact and create a plan of action.

Data Localization

Michael Nelson with CloudFlare summarized the breakout session on data localization. Participants discussed differences in the international landscape on the issue. For example, in some cases, countries might want to keep data close because of reasons having to do with enforcing privacy protections, extending or limiting law-enforcement access, and protecting national industries. The group also discussed the arguments and counter-arguments around data localization (e.g., is distributed data less protected, are smaller countries less protected, and is it advantageous to reduce the size of targets for cyberterrorists?).

Potential next steps proposed by the group included developing case studies (house monitoring, medical devices that travel with users, efficient routing, etc.); gathering economic analysis and performing technical analysis; exploring certification for data practices and where, for example, IEEE might be able to develop adequacy checklists for educating governments; and surveying where policy is being written and in what areas that additional education is necessary.

Education and Ethics

Emily Nichols with Internet2 reported that the education and ethics breakout session focused on four possible next steps: developing content and programs for education and ethics around IoT, identifying partner channels for creation and distribution of content, determining performance indicators, and assigning an implementation owner. The group suggested IEEE as the owner of programs for education and ethics around IoT because of the organization’s proven range of services in the space and technological and global scope.

Content could address engineering ethics and the TIPPSS attributes; reflect multiple generational viewpoints on privacy, sharing, and trust; and incorporate meaningful iconography and/or be embedded in gaming environments to creatively demonstrate concepts. Ms. Nichols also detailed a list of possible partner channels that the group envisioned, including

- Diversity and industry organizations,
- Community organizations,
- Schools,
- Teacher unions,
- Philanthropic organizations,
- Libraries,
- Do-it-yourself/maker communities,
- Industry partners, and
- Professional trade associations and certification organizations.

Conclusion

In addition to the suggested next steps from the breakout sessions in data localization, education and ethics, end-to-end security/privacy by design, and technology policy development process, this IEEE ETAP Forum concluded with co-moderator and IEEE Internet Initiative Chair Oleg Logvinov's challenge to participants to continue the conversation in the weeks ahead. He asked participants to elaborate on the issues they voiced during the rapid-fire brainstorming earlier in the day into one- or two-paragraph explanations that would more broadly outline concerns and potential actions. Mr. Logvinov suggested that the explanations might spark an even more wide-ranging global conversation and cross-pollination of ideas on privacy, cybersecurity, and Internet governance, leading into the next regional IEEE ETAP Forum gatherings, which are scheduled for 4 March 2016 in Delhi, India, and 17 May 2016 in Beijing, China.

"Eliminating the gap between technology and policy entirely probably will not be possible for some time," Mr. Logvinov said. "But, at least, if we can start closing that gap, we will have made a very positive and very important step forward."

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 Washington, D.C., USA, on 5 February 2016 was the third 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. More than 50 diverse stakeholders from around the world—government and industry representatives, legal practitioners, and academics—gathered at The George Washington University for the one-day event organized by the IEEE Internet Initiative.

Location: Marvin Center at The George Washington University

Moderators: Oleg Logvinov and Clint Andrews

Oleg Logvinov

After graduating from the Technical University of Ukraine (KPI) with the equivalent of a Master's degree in electrical engineering, Oleg Logvinov worked as a senior researcher at the R&D Laboratory of the Ukraine Department of Energy at the KPI.

During the last 25 years Mr. Logvinov has held various senior technical and executive management positions in the telecommunications and semiconductor industry. He currently serves on the IEEE IoT Initiative Steering Committee and is the past member of the IEEE Standards Association (IEEE-SA) Standards Board and the IEEE-SA Corporate Advisory Group. In January of 2015 Mr. Logvinov was appointed as the chair of IEEE Internet Initiative. The IEEE Internet Initiative connects engineers, scientists, industry leaders, and others engaged in an array of technology and industry domains globally with policy experts to help improve the understanding of technology and its implications and impact on Internet governance issues. In addition, the Initiative focuses on raising awareness of public policy issues and processes in the global technical community.

Mr. Logvinov also actively participates in several IEEE standards development working groups with the focus on the IoT and communications technologies. Mr. Logvinov is the chair of the IEEE P2413™ Internet of Things (IoT) Architecture Working Group. He helped found the HomePlug Powerline Alliance and is the past President and CTO of the Alliance. Mr. Logvinov has 24 patents to his credit and has been an invited speaker on multiple occasions.

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, is a past member of the Board of Directors of the IEEE and the International Society for Industrial Ecology, and a winner of the IEEE's 3rd Millennium Medal. His books include *Industrial Ecology and Global Change*, *Regulating Regional Power Systems*, and *Humble Analysis: The Practice of*

Joint Fact Finding.

Start Time	**End Time**	**Program**
8:15 am	9:00 am	*Network and continental breakfast*
9:00 am	9:15 am	*Introductions* Oleg Logvinov
9:15 am	9:35 am	*Keynote Presentation — Technical* **Designing Privacy into Internet Protocols** Juan Carlos Zuniga Juan Carlos Zuniga is a Principal Engineer at InterDigital, where he leads the standardization activities on virtualization (NFV/SDN), dense and heterogeneous wireless networks (cellular, Wi-Fi, IoT), content management, and Internet privacy. He has held leadership roles and contributed in different standards fora, such as IEEE 802, IETF, ETSI, and 3GPP. He is co-chair of the IETF Internet Area working group and ex-chair of the IEEE 802 Executive Committee Privacy Recommendation study group. Previously, he worked with Harris Canada, Nortel Networks UK, and Kb/Tel Mexico. Juan Carlos received his engineering degree from the UNAM, Mexico, and his MSc from the Imperial College London, UK. He has several publications and has been guest editor for the IEEE Communications Magazine. Juan Carlos is inventor of over 50 granted patents.
9:35 am	9:55 am	*Keynote Presentation — Policy* **Achieving a Secure and Resilient Cyber Ecosystem: A Way Ahead** Thomas Ruoff Director of Innovation for the Chief Technology Officer with the U.S. Department of Homeland Security

Start Time	End Time	Program
10:00 am	10:55 am	*Panel* **Overview of issues highlighted at the IEEE End-to-End Trust and Security for the Internet of Things Workshop** Oleg Logvinov (moderator) Mark Cather Florence Hudson Richard Bennett Robert Martin Susan Hyon Parker
10:55 am	11:05 am	Break
11:05 am	12:00 pm	*Panel* **Privacy, security, and innovation challenges in different aspects of IoT** Oleg Logvinov (moderator) Carl Landwehr William Whyte Saifur Rahman Glenn Fink Ekaterina Rudina
12:00 pm	12:30 pm	*Rapid-fire round-up of key issues from all participants* Clint Andrews
12:30 pm	1:15 pm	**Lunch**

Start Time	**End Time**	**Program**
1:15 pm	1:45 pm	*Review and comparison of previous ETAP Forum outputs and discoveries* • ETAP San Jose 2015 • ETAP Tel Aviv 2015 Jared Bielby Jared Bielby received a double master's degree from the University of Alberta, Canada, in information science and digital humanities with a thesis route in the field of information ethics. He works as an independent consultant in information ethics and Internet governance. He currently serves as co-chair for the International Center for Information Ethics and editor for the International Review of Information Ethics. He is moderator and content writer for the IEEE Collabratec Internet Technology Policy Forum and is founder and editor-in-chief of *The Freelance Netizen*. His research and writing looks at the interdisciplinary connections between information and communication technologies (ICTs) and information ethics, digital citizenship, and culture. Bielby has written and spoken internationally on subjects of information ethics, Internet governance, and global citizenship in a digital era.
1:45 pm	2:00 pm	*Synthesize and refine selection of highest priority issues* Clint Andrews
2:00 pm	2:50 pm	*Breakout Session* *Delve deeper into highest priority issues*
2:50 pm	3:00 pm	*Break*
3:00 pm	3:30 pm	*Report-outs from breakout teams* Volunteer breakout leads
3:30 pm	4:00 pm	*Next steps, action plan and wrap up* Clint Andrews

Appendix II: Participants

Oleg Logvinov, Chair, IEEE Internet Initiative; Chair, IEEE P2413 Internet of Things (IoT) Architecture Working Group

Clinton Andrews, Rutgers University

Ed Aractingi, Marshall University

Richard Bennett, Consultant

Jared Bielby, International Center for Information Ethics

Mark Cather, University of Maryland Baltimore County

Alan Chachich, U.S. Department of Transportation

Srikanth Chandrasekaran, IEEE India

Miwako Doi, National Institute of Information and Communications Technology

Glenn Fink, Pacific Northwest National Laboratory

Rob Gingell, Resilient Network Systems

Chris Hrivnak

Peizhao Hu, RIT

Florence Hudson, Internet2

Susan Hyon Parker, Carnegie Mellon Open Learning

Chris Jannuzzi, IEEE

Walter Kawula, Hahn Loeser Parks LLP

Carmen Kocinski, self

Semen Kort, Kaspersky Lab

Carl Landwehr, The George Washington University

Margaret Loper

Randolph Marchany, Virginia Tech - VPIT/ITSO

Robert Martin, MITRE

Satyajayant Misra, New Mexico State University

Martin Murillo, University of Notre Dame

John Murray, SRI International

Eric Nance Woehler, Interprose

Michael Nelson, CloudFlare

Nicole Newmeyer, National Security Agency

Emily Nichols, Internet2

Mary Lynne Nielsen, IEEE

Karen O'Donoghue, Internet Society

Saifur Rahman,Virginia Tech

Raghuraman Rajanarayanan, Achronix Semiconductor

J. Scot Ransbottom, Virginia Tech

Sumitra Reddy, West Virginia University

Ramana Reddy, West Virginia University

Ekaterina Rudina, Kaspersky Lab

Thomas Ruoff, U.S. Department of Homeland Security

Anna Slomovic, Consultant

Brian Stengel, University of Pittsburgh

Robert Stien, InterDigital

Kristene Unsworth, Drexel University

Steve Wallaces, Indiana University

Pamela Weedon, Interprose

James Wendorf, IEEE

William Whyte, Security Innovation

Stephen Wolff, Internet 2

Ting Zhu, UMBC

Viacheslav Zolotnikov, Kaspersky Lab

Juan Carlos Zuniga, InterDigital Labs

Appendix III: Rapid-Fire Brainstorming

Participants at the Washington IEEE ETAP Forum listed their individual priorities in a rapid-fire brainstorming session:

- Standards to allow for trust across propriety systems
- Effect on privacy and civil rights through algorithms
- Our overlapping persona using the same IoT tool
- Building a foundation that is flexible and scalable
- How to teach students when they are building systems
- Articulating the policies that will govern this
- Recognizing human autonomy in an IoT world
- Authenticity of global standards organizations
- How to communicate IoT priorities for security and privacy to developers and industry so that can be shared with clients and customers
- Identity management and its relation to security and policy from a human perspective (neurological and interaction with systems)
- Privacy-related policy gaps that can be closed quickly: what are they?
- How do we provide technical needs for accountability in IoT data flows?
- How do we educate the public about this, and what is the role of engineers in this?
- Education and need for preparing future professionals about privacy and security
- A framework for instilling ethics development for current and future generations
- How do we ensure edge devices are trustworthy and secure?
- How to ensure end-to-end security from design to fabrication across the supply chain for devices?
- How to address the financial/cost concerns to create trust and security in products?
- Need for international collaboration on cybervulnerabilities versus the impact on privacy concerns and national considerations (e.g., Fossenar agreement)

- Keep TIPPSS in mind

- Analytics being used as a privacy veil and also as a tool that breaks the privacy veil

- Data localization yet moving data across national borders: which legislation applies?

- How do we handle a hack that also exposes a crime?

- Need guidelines and standards on privacy by design

- How do we build ways to address the questions on IoT and privacy/security and create usable outcomes?

- International economy of data: when data becomes the currency of corporations and nations, how do we connect the sources of data to this economy so they may benefit from it?

- How do we facilitate the development of privacy-preserving policies for IoT?

- Allowing for innovation that has yet to happen in what we create through today's policies

- Tech drives legal and policy, and the need to make technologists aware of that

- A forward-looking roadmap related to US Constitution's 4th amendment search and seizure in an IoT world

- The future is here and we still don't know what to do with it: adjusting the great technical solutions to the practical and evolving needs of the market and the attendant policy needs for secure solutions

- Need descriptions of properties of different domain areas to see where the similarities and differences are

- Legacy systems that can't expand to encompass IoT needs, particularly critical systems

- How regional policies affect global trade

- How do we bring different policy makers in different regions together to discuss IoT issues?

- Education on ethics needs to happen in the public schools (pre-college) to inculcate certain principles

- IoT issues relate to existing problems in sensor networks: what can be examined there and repositioned?

- Data localization is important for IoT and the future Internet

- Avoid unconscious technological lock-in through dominant players and/or existing case law

Appendix IV: Top 10 Issues

The issues voiced during the rapid-fire brainstorming session at the Washington IEEE ETAP Forum were clustered into 10 topics for consideration of targeted breakout sessions:

- Education
- Data localization
- Identity management
- Technology policy development process
- Autonomy
- Accountability
- Tradeoff adjudication
- Solutions roadmap creation
- Ethics
- End-to-end security/privacy by design

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

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