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

SCOPING THE GAP BETWEEN TECHNOLOGY AND POLICY

SAN JOSE, CA, 18 MAY 2015

VERSION: 4 AUGUST 2015

IEEE

Contents

IEEE Experts in Technology and Policy (ETAP) Forum on Internet Governance, Cybersecurity, and Privacy: Scoping the Gap between Technology and Policy

Executive Summary

The ongoing effort by technologists to create standards-based, global technology solutions for cybersecurity and data privacy often conflict with or challenge regional and national policies around the world. Technologists and policymakers often occupy different realms of the Internet governance ecosystem, which limits mutual understanding of each other's domains, perspectives and challenges. Yet the current state of Internet governance, coupled with frequent breaches in cybersecurity and data privacy, lends urgency to the search for solutions to the gaps between technology and policy in Internet governance.

The IEEE Internet Initiative was launched in 2014 as a neutral platform to connect technologists and policy makers to better inform both sides as they work to close these gaps. The Initiative also seeks to provide insights to policy makers on the trade-offs inherent in various policy choices regarding technology.

IEEE has a unique role to play in resolving gaps between technology and policy in Internet governance due to its scale, ubiquity, geographic and technical diversity, its convening power, its open and transparent processes and its ability to provide a neutral platform for resolving issues. To make an effective contribution in this realm will require IEEE to leverage resources across its global membership, technical communities and programs to include non-technology elements such as ethics, law, culture and real-world, market conditions.

This paper documents the discussions and outcomes of an IEEE forum, "The Experts in Technology and Policy (ETAP)," whose purpose is to identify and articulate high-priority issues in Internet governance, cybersecurity and privacy. The inaugural ETAP Forum was held in San Jose, California, on 18 May 2015. ETAP participants included representation from China, India, Africa, Europe, Canada and the United States. The process identified 20 priority issues (see Appendix II). The following six were deemed high priority:

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.

Introduction: IEEE Internet Initiative

The promise and future of the Internet faces a fundamental challenge: how can technologists design standards-based global technologies for the Internet, including technologies that enhance cybersecurity and data privacy, when adoption of those standards and technologies remains the purview of regional, national or even local authorities?

This conundrum, if unresolved, has the potential to fragment the Internet and its governance, divide the global community of Internet users and undermine confidence that the global network works as intended for everyday communications, commerce and innovation in myriad domains.

Fragmentation limits economies of scale, stymies market growth and, thus, inhibits Internet access and affordability for the world's approximately nine billion people – half of whom currently do not access the Internet. The nascent Internet of Things, which promises a world of connected people, devices and data for efficiencies, productivity and innovation, heightens the urgency of addressing and resolving gaps between Internet technology and policy.

A growing realization that the so-called "Internet governance conundrum" could benefit from intentional, organized, global collaborations between technologists and policy makers led, in part, to the 2014 formation of the IEEE Internet Initiative. IEEE recognizes that other global technology and policy organizations are currently at work on roughly parallel efforts, but IEEE also sees an opportunity to leverage its many unique attributes to contribute to the resolution of the issues outlined in this paper.

The IEEE Internet Initiative's mission to promote technically sound policy to fuel Internet innovation, sustainability and market growth provided an opportunity for IEEE to launch the "Experts in Technology and Policy" (ETAP) forum to provide a neutral platform for technologists and policymakers to share mutually pertinent insights.

Inaugural ETAP Forum Invited Speakers

The format for the first ETAP Forum was designed to inform and inspire participants with technology, policy and international perspectives prior to asking them to name their most important Internet governance issues, vote on those needing the most attention and work in break-out groups on defining those issues.

Peter Fonash, CTO for the U.S. Department of Homeland Security, primarily addressed efforts to secure critical infrastructure in the United States and the need for collaboration between industry and government to meet cybersecurity threats. Deepak Maheshwari, head of government affairs for Symantec (India), discussed Internet use in an emerging economy and the issues of access, affordability and cultural differences in user perspectives on cybersecurity and data privacy. Xiao Dong Lee, CEO/CTO for the China Internet Network Information Center (CNNIC), provided his agency's perspective on Internet challenges and technology solutions. Jessica Groopman, a market analyst with Altimeter Group, characterized the consumer perspective on the Internet of Things (IoT), which touched on Internet governance issues, including cybersecurity and data privacy.

A five-person panel convened speakers from academia, industry, government and non-governmental organizations (NGO). Jared Bielby, co-chair of the International Center for Information Ethics, a virtual, global platform for discussion, brought a philosopher's perspective to the panel. Nancy Cam-Winget, a distinguished engineer for Cisco Systems, lent a security architect's view to the discussion. John Cioffi, CEO and chairman of ASSIA (Adaptive Spectrum and Signal Alignment, Inc.), provided a view honed in both academia and industry. Stephen Diamond, general manager, Industry Standards Office, and global standards officer, Office of the CTO at EMC, offered decades of industry experience. Greg Shannon, chief scientist for the CERT Division at Carnegie Mellon's Software Engineering Institute, and chair, IEEE Cybersecurity Initiative, offered industry, academic and NGO experience and perspective.

Discussion

The highlights of these speakers' and panelists' contributions to the ETAP discussion follow in the next section of this paper.

Speakers and Panelists

As this paper is designed as a foundational document in the ETAP Forum process, its intent is to stimulate discussion rather than determine outcomes. Thus this paper includes accounts of the invited speakers' main points and a sense of the discussion generated by the invited panel to provide breadth and context to the high-priority issues identified by Forum participants.

Peter Fonash, CTO for the U.S. Department of Homeland Security (DHS)

Fonash had responsibility for restoring communications in New York after the terrorist attacks on 11 September 2001 and in Louisiana after Hurricane Katrina in 2005. Today he is CTO for cybersecurity and communications for DHS, which he said allows him to be proactive about future challenges. At ETAP, Fonash first described three activities that protect government agencies. The Einstein Program is an intrusion detection program for monitoring network gateways used by government agencies. The Trusted Internet Connections Initiative limits the number of Internet connections used by the federal government and filters related traffic. The Continuous Diagnostics and Mitigation Program provides cybersecurity tools for each agency's environment to assess assets and vulnerabilities.

Fonash then discussed DHS' ongoing challenges in meeting the government's cybersecurity needs.

"We're recognizing that we're having problems doing cybersecurity," Fonash said.

First, there's a shortage of skilled workforce to perform cybersecurity, which is getting worse. The U.S. government runs a scholarship program to mitigate the shortage. Second, there are no cybersecurity data standards, which cause issues for interoperability, reduces analyst productivity, and causes delays. Third, the effectiveness of detection and mitigation efforts is not optimal.

In fact, Fonash said, quoting 2014 Verizon data, in 2003 the "good guys" could detect a cyber-intrusion about 20 percent of the time, in a day or less. The "bad guys" were able to get in and get out 70 percent of the time, in a day or less. Today, the "good guys" can detect a cyber-intrusion about 25 percent of the time, in a day or less, yet the "bad guys" get in and get out 90 percent of the time within a day or less.

"We were doing badly in 2003 and we're doing worse today," Fonash said. "So we need to do some paradigm shifts here."

"On top of that you have the Internet of Things," Fonash continued. "We were doing poorly with managed networks. We have actually a whole organization set up to do security for [managed networks] and we can't protect [them]. Just think what's going to happen with the Internet of Things."

The "cyber-ecosystem" – the combined domains of Internet, people, processes and technology – means "we're all bound together by interconnections," Fonash said.

He cited a paper published in 2011, written by Philip Reitinger, former deputy undersecretary for the National Protection and Programs Directorate (NPPD), DHS, titled, "Enabling Distributed Security in Cyberspace: Building a Healthy and Resilient Cyber Ecosystem with Automated Collective Action."

"That holistic environment means we all have the same cybersecurity problems and we have to address them as a group," Fonash said. "We can't address [cybersecurity] individually, for many reasons. For one thing, we all have supply chain problems. Target is a great example. Its HVAC supplier was the venue by which [a well-publicized 2013] attack was propagated."

"We also need innovation, which we don't do as quickly as we should," Forash continued.

Three components of the cyber-ecosystem need addressing in DHS' view, according to Fonash. One is the enterprise architecture, whether that's enterprise IT, the cloud, or process control systems.

"For instance, [DHS worries] about process control systems, because we protect critical infrastructure," he said.

"That cyber-ecosystem will also need tools and capabilities" to sense attacks, determine a course of action and take action, he suggested. Those tools and capabilities probably will need to be automated, for speed. This area remains in its infancy, however, and some warn of unintended consequences.

The second component is the concept of a "cyber weather map," which gathers cyber incident and reputational information, performs analytics and outputs the results via visualization tools.

The third component is an information infrastructure that can share information in "cyber-relevant time," driven by automation.

Summarizing the technology needs of the cybersecurity challenge for critical infrastructure, Fonash said:

"We need interoperability of tools. Right now we have individual tools, [but] they're not tool sets. We need those tools in a shareable format, so that everyone understands them. Once we have interoperability, then we can move to automation – automated courses of action. And we need a trust mechanism to share information.

"A trust mechanism has two pieces," Fonash said. "The first is authentication, so I know who I'm sharing information with. But also trust in the sense of a partnership, [so both sides trust each other's integrity]. Once you have interoperability, automation and trust, you can get to information sharing, so that people can learn from each other's mistakes, experiences and practices."

All of these practices and processes should fit within a risk management framework for the full cybersecurity lifecycle (identify, protect, detect, respond and recover), Fonash said.

"The bad news in all of this is that cybersecurity isn't going to be solved," Fonash concluded. "We get better, the adversary gets better."

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

Maheshwari placed India and its challenges in context by pointing out that it is the second most populous nation in the world, with the second largest set of Internet users. More than 300 million people in India use the Internet, yet the country has 1.2 billion people. Thus three out of four Indians do not use the Internet due to issues with access and affordability. Usability is challenging as well, based on the country's linguistic and cultural diversity. And notions of data privacy and security are disregarded by some in favor of access to value.

India's linguistic and cultural diversity pose significant challenges to Internet uptake, according to Maheshwari. In the European Union, which has 28 member countries, for instance, a common homepage offers 24 language options. In contrast, in India, 22 official languages are currently used (apart from English) and many hybrids exist. Numerous languages are shared with neighboring countries. One language may use multiple scripts and multiple languages may use the same script. Some languages flow left to right, others, right to left. Perhaps 15 percent of the population is proficient in English.

The means of access for those who use the Internet is increasingly mobile, Maheshwari said. India has 950 million mobile accounts among 650-700 million users (due to multiple SIM (subscriber identity module) cards) and two-thirds of those accessing the Internet do so exclusively via mobile devices. (Perhaps 27 million landline connections exist – a number that is rapidly shrinking – for India's 1.2 billion people.) As much as 95 percent of mobile accounts in India are prepaid. Two-thirds of India's population lives in rural areas, however, which are insufficiently covered by cellular networks.

India's service-based economy accounts for two-thirds of gross domestic product (GDP), though half of working Indians toil in agriculture. Thus India has a service economy but an agrarian society. Average annual income in India is ~$1,500.00. Perhaps 300 million people live on less than $2 per day, according to Maheshwari. So the cost of Internet-related devices and access remains a significant expense for many of India's people.

"Within that context, a lot of users do find value in the usage of mobile and the Internet," Maheshwari said. "It is in this context that we must look at how policy and regulation plays a role... About fifteen years back, we began a number of programs and policies to encourage Internet use to empower people."

India's leaders sought a path to "inclusive, equitable and sustainable development," Maheshwari said. "Sustainable" means not just environmentally, but also with respect to economic growth, he added. Efforts at economic sustainability include "Digital India," a $19 billion plan launched in 2014 that relies on three pillars: ubiquitous broadband, delivery of government services via technology and digital empowerment of the citizenry, particularly in education and healthcare. The challenge: two-thirds of the country's population lives in rural villages. An initial technology focus on fiber optic cable has given way to a technology-neutral stance for cost-effectiveness and flexibility. Satellite-, balloon- and cellular-based broadband options are among the possibilities under discussion, Maheshwari said.

On the user side, soft keyboards and rich audio-visual content have, to a degree, mitigated the linguistic challenges posed by a text-heavy Internet, he added.

On the policy front, a number of India's unique attributes have raised a variety of issues, according to Maheshwari.

Because ICT (information and communications technology) did not exist when India wrote its constitution in the late 1940s, ICT-related regulation exists at the state level and, thus, is fragmented, Maheshwari said. Though the nation's Information Technology Act provides over-arching legislation, the central government and states continue to frame additional policies.

Tension has arisen between preserving "freedom of expression" on the Internet while discouraging or outlawing "grossly offensive" online content, Maheshwari said. A law barring "grossly offensive" content had the perhaps predictable if unintended consequence of pitting adversaries against each other in court and, after explosions in litigation, the law was rescinded by India's Supreme Court in March 2015.

The Indian government has established a public-private sector working group for cybersecurity; a senior official in the Prime Minister's office serves as National Cyber Security Coordinator. India is supportive of a multi-stakeholder model of Internet governance, Maheshwari said.

Though India claims 60 percent of the world's outsourcing, its success relies on the free flow of data. Yet government agencies have periodically set limits on the level of allowable encryption to maintain throughput, which may compromise security.

In a rough analogy to people elsewhere, India's citizens have demonstrated a willingness to set aside concerns about data privacy and security in exchange for value – a characteristic perhaps enhanced by the relative poverty of many citizens. In one outreach effort, the government encouraged the adoption of bank accounts by taking advantage of widespread mobile telecom use and the ability of SIM cards to facilitate financial transactions. The biometrics of program participants are recorded by third parties and stored by the government, yet the resulting biometric cards are immensely popular because they also serve as the means to receive valuable entitlements, Maheshwari said. In six years, 800 million users have enrolled and growth continues at a pace of one million enrollees every day. It appears that the value of the entitlements induces participants to set aside concerns about data privacy and security, Maheshwari concluded.

Xiao Dong Lee, CEO/CTO, China Internet Network Information Center (CNNIC)

Lee addressed a broad range of Internet governance issues, particularly the gap between technology and policy making.

"Even if you have a perfect technical solution, without the policy solution, it cannot be deployed," Lee said. "If you have a very good policy, but no technical solution, it means nothing."

Three critical philosophical questions that govern use of the Internet and related privacy and security issues, according to Lee, include: Who are you? Where are you from? Where do you want to go? These questions track to the practical challenges of managing the Internet domain name system (DNS), IP addressing and AS (autonomous system) routing.

"If we totally understand and can manage those three issues, then we can manage the whole Internet," Lee suggested.

In terms of recent events related to these Internet governance issues, Lee cited the NTIA's (National Telecommunications and Information Agency, U.S Department of Commerce) March 2014 announcement that it would ask ICANN (Internet Corporation for Assigned Names and Numbers) to develop a proposal to convene a global, multi-stakeholder community to determine how NTIA could transition its role in coordinating the DNS to that multi-stakeholder community. This has led to further discussion of how the U.S. government can be induced to give up control of ICANN because of the latter's dominant role in Internet naming, addressing and routing.

Though Lee stipulated that he spoke at ETAP as an individual, he described his organization – China Internet Network Information Center (CNNIC) – and its work. Established in 1997, CNNIC is an important, nonprofit constructor, operator and administrator of critical infrastructure for China's Internet, including research and security roles.

"Almost every country has a similar organization to manage domain names, IP (Internet Protocol) addresses and AS (Autonomous System) numbers," Lee said. "We try to create a stable and secure system for China. Perhaps half of all websites in China are built on a [CNNIC-aided] platform. This is critical infrastructure for China."

"CNNIC has a very close relationship with the government," Lee continued. "In China there is no real nonprofit organization. Every 'nonprofit' must be hosted by the government or some governmental organization. We also have a very close relationship with industry. We provide the technology to the [business] community to improve the whole [Internet] infrastructure for China. We also work as a policy coordinator. We try to connect industry with the government to meet the gap between the technical solutions and the policy makers."

Lee listed several hot topics in naming and addressing technologies, including domain naming.

"The first thing is 'internationalization,'" he said. "We also call that 'localization.' Because now, in China, there are 650 million Internet users [in a population of approximately 1.4 billion], but most of them are not familiar with English. We have another 650 million people who are not connected to the Internet. How can we make sure they can access the Internet? We need to build a multi-lingual, localized way for them. For internationalization, it is very difficult to solve that."

"Another issue is internationalized email addresses," Lee said. "Email is a killer application for [the] Internet. We have proposed a standard before the IETF (Internet Engineering Task Force) for internationized user names in email addresses. But now that the standard is finished, the next step is how to solve the issue for the application [itself]."

Lee discoursed on security issues by mentioning DNSSEC (Domain Name System Security Extensions) as an example.

"It is not new technology," Lee said, but still, hackers can intercept e-commerce transactions, for instance, that rely on it.

"This is a typical issue for the gap between technology and policy," Lee said. "DNSSEC is a technical solution, a perfect solution. But even though we've had this solution for over two years, no one can make a perfect policy that will push everyone to deploy it."

Lee also discussed ongoing issues in addressing and routing.

In conclusion, Lee pointed out that China has enacted several privacy protection laws, including limiting Internet access by minors and penalties to curb the spread of malicious information. However, he noted, there exists no perfect technical solution to support those policies.

That leaves the focus on how technology can inform policy, he suggested.

"A globalized technology solution can improve policy making and implementation," Lee concluded.

Jessica Groopman, market analyst, Altimeter Group

Groopman provided a strong contrast to the technology angle by bringing consumer-centric, policy-related issues to the fore in a talk titled, "Consumer Perceptions of IoT (Internet of Things)."

To illustrate the stakes in consumer perceptions of privacy in an interconnected world, Groopman quoted from a 2015 Federal Trade Commission staff report, "Internet of Things, Privacy & Security in a Connected World":

“The perceived risks to privacy and security, even if not realized, could undermine the consumer confidence necessary for the technologies to meet their full potential and may result in a less widespread adoption.”

In fact, this lack of adoption due to privacy concerns is already documented, Groopman noted.

A 2014 survey by the Acquity Group, an e-commerce and digital marketing group, asked respondents why they haven’t purchased a connected, in-home device. Thirty-four percent said they did not understand the value and 23 percent mentioned privacy concerns.

“This is a call for value, and trust,” Groopman said.

Further, a Nielsen survey found that of consumers who have heard of IoT, 53 percent said their top concern is that their data may be shared without their knowledge or approval.

Groopman suggested that recent news of data breaches, from Edward Snowden’s revelations about the National Security Agency’s surveillance programs to Facebook’s surreptitious research on users’ emotional reactions to content in the name of improving the user experience, have undermined consumer confidence that online activities are private. In fact, 42 percent of people surveyed by TRUST-e, an online privacy management service, are more worried about their online privacy than they were just one year ago, Groopman noted.

According to a recent survey by Altimeter Group, understanding and trust in how companies use consumer data is low, but interest in online services and connected devices remain high, Groopman said. A recent TRUST-e survey found that close to 9 out of 10 consumers want to understand more about personal data collection before they buy a connected device and a similar proportion want control over that data.

Two other dynamics appear to be at play in consumer perception, Groopman said.

One is that research shows that the greater a consumer’s involvement with technology (measured by the number of connected devices they use), the more they report greater understanding, trust and interest in how companies use their data. The other dynamic is captured by the anecdotal observation by a respondent in Groopman’s research who said, “If the value is there, consumers will share” – an attitude that may well reflect the current, uneasy consumer stance towards using search engines, websites and online services despite not knowing whether or how their personal behavioral data is being used or even sold.

“Value” appears linked to savings in time, effort/energy and money, Groopman said. She suggested that consumer-facing businesses will find an opportunity to differentiate themselves by providing feedback to consumers on how data is collected, used and/or shared.

Gaps remain between consumer perception and knowledge and what consumers say they want, Groopman said.

Currently, consumers lack knowledge, awareness, understanding, consent, control, comfort and trust, she said. And they have a desire for visibility, education, “intervenability,” agency, reassurance and value.

How will commercial interests respond to this state of affairs? Groopman asked rhetorically.

“There’s a long way to go,” she said. “The default today in terms of how companies share and communicate with consumers on how their data is being used is provided in the ‘terms of service’ that nobody actually reads.”

In response to the foregoing points, Groopman presented “four pillars of business communications for ethical data use”:

- Consumer education (“Be a partner with consumers, don’t be a spy.”)
- Transparency and disclosure (“Accountability. What is a company going to do with a consumer’s data? What about transferring data to partners and third parties?”)
- User control and intervenability (“Build trust.” The binary choice of opt-in or opt-out should be replaced by a gradient or menu of options. Allow users the ability to choose what they want to share, when, and with whom.)
- Value exchange (“Ask for feedback. Advance the conversation.” Clearly articulate what service or value is provided to consumers to induce them to share their data. E.g., “If you give us ‘x,’ we’ll give you ‘y.’”)

In closing, Groopman quoted Gilad Rosner, founder of the Internet of Things Privacy Forum:

“The tectonic shifts we’re seeing in technology are not matched by such dramatic shifts in human behavior. Culture, values, norms, politics, how we interrelate with one another – these things change slowly.”

The Panel Discussion

Each of five panelists was given the opportunity to express their view on the most important Internet governance issue(s) needing attention as the ETAP Forum process progresses.

Jared Bielby, co-chair of the International Center for Information Ethics, a virtual, global platform for discussion, described his background in information ethics and his interest in examining and questioning the inter-cultural implications of Internet governance work by national or global organizations.

For instance, Bielby said, does the concept of “multi-stakeholder” consensus truly represent involvement by the voiceless? An argument can be made, he suggested, that many action-oriented Internet governance organizations are biased toward commercial interests.

“Everyone should be stakeholder, if they so wish,” Bielby said.

He acknowledged that this goal is hindered, in many instances, by a lack of citizen engagement, education, human rights and economic clout. He urged ETAP participants to maintain an open definition of privacy and security and to ensure that their work addressed human rights for the Internet.

Nancy Cam-Winget, a distinguished engineer for Cisco Systems who works in security architecture, suggested that major challenges remain in resolving tensions between desired qualities in Internet governance. The urgency in addressing these tensions is driven partly by estimates that the Internet will connect 50 billion “things” within the next five years.

“One thing I haven’t heard [discussed today] is the tension between security, privacy and safety,” she said. “That brings [up] discussion of improving the efficacy of threat detection and sharing information without – when we’re talking about critical infrastructure – leaking intellectual property.”

Cam-Winget also touched on the physical threat posed by the potential to weaponize critical infrastructure – a nuclear plant, an airplane – against people.

She also mentioned the tension between data anonymization and efficient data flows on a network. As privacy and security measures improve, the functionality of networks must be preserved.

Reputational models may help users avoid Internet-based threats to data security, but so far no technology or policy can provide assurance or proof that data anonymization has taken place, she added.

John Cioffi, CEO and chairman of ASSIA (Adaptive Spectrum and Signal Alignment, Inc.), asked participants if they'd had an Internet connection problem recently. Nearly everyone raised their hand.

"What do consumers really want?" Cioffi asked. "They want [the Internet] to work."

"How do we know that things are working, vis-à-vis privacy, security and all the issues we're discussing?" he asked rhetorically.

Citing a Federal Communications Commission report that the Internet works for most people 80 percent of the time, with 80 percent of expected performance, he said that leaves significant performance issues unaddressed.

"[If] your Internet connection [doesn't] work, what do you do?" he said. "You want it to work, your applications to flow. You don't want to worry about security, but you don't want to be harmed. Most of you are having a problem getting what you want out of the Internet without having a security problem per se. But all these factors have to work together."

Stephen Diamond, general manager, Industry Standards Office, and global standards officer, Office of the CTO at EMC, addressed a "meta-issue."

The problem we face is that technology is beneficial when its benefits outweigh its costs, Diamond said. He suggested that Internet governance work should not overlook what he called the "third Internet" – the cyber-physical systems whose manipulation could result in physical destruction and injury to people. (For example, industrial control systems (ICS).) It's possible that costs will outweigh value, if certain issues are not resolved. But people and institutions are not particularly good at dealing with the current scenario in which the Internet is a global, unmanaged network, he said.

"These systems that we are unleashing on ourselves and on the world were not designed from the top down, which is how you'd want to design a system with such potential for ill, as well as good," Diamond said.

IEEE offers a unique substrate for the path to solutions, he said. But the benefit must clearly exceed the cost. The Internet governance challenge plays to IEEE's strength as a neutral arbiter of technology choices and their trade-offs and outcomes.

"These [cost-benefit crossover trends] are accelerating and we're running out of time," Diamond said.

Greg Shannon, chief scientist for the CERT Division at Carnegie Mellon's Software Engineering Institute, and chair, IEEE Cybersecurity Initiative, suggested that solutions may require a similar timeframe to that in which challenges arose.

"Fundamentally, I'm optimistic, but I'm a realist," Shannon said. "It took us 45 years to get here."

Ten years ago, policy makers saw that the Internet offered an engine of innovation and created multi-billion-dollar companies and they paid insufficient attention to security and privacy challenges, which now demand resolution – particularly with the universal connectivity promised (or threatened) by the Internet of Things, Shannon said.

In terms of advancing technology, the challenge is to ensure that we can confirm the efficacy of privacy and security measures, he suggested. This is possible today, but it requires orders of magnitude greater computing power than is commonly available.

We should find technology opportunities to create barriers to existential threats, such as Internet-based manipulation of industrial control systems that could lead to mass destruction and death, Shannon suggested.

He also noted that the multi-stakeholder model for Internet governance crumbles when manipulated by actors who ignore the trust model on which Internet governance policies often are based, Shannon said.

Results: ETAP Forum Outcomes

The ETAP process in San Jose was designed to inform and inspire participants with the speakers and panel described above, and then to identify the most important Internet governance issues. Twenty (20) issues were identified, then reduced to six high-priority issues.

The six top issues and the accompanying discussions that arose in related break-out sessions are summarized here. Each group was assigned an issue and asked to address four questions in their deliberations:

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

1. Data analytics

Data analytics can be a powerful tool for the benefit of humanity, but it has risks and unintended consequences. An effort by the U.S. state of Massachusetts to release anonymized health data for research purposes backfired when an Massachusetts Institute of Technology graduate student combined the data with voter registration records and re-identified more than 80 percent of the people in the purportedly anonymized data set. The mathematical models needed for anonymizing data are very complicated, but that doesn't mean we shouldn't try.

International consistency? No. Most laws are based on the concept of notice and consent but vary widely across the globe. And policies and regulations can be fragmented. In the U.S., e.g., notice and consent rules vary by sector, with different rules for healthcare, finance, etc.

Key stakeholders? Everyone. Individuals, enterprises, government/regulators.

What could the IEEE do in this area? Develop a standardized approach for guaranteeing anonymity.

2. Multi-stakeholder governance

Governments alone should not be left to this task. It should include "all of us." The group cited the ICANN (Internet Corporation for Assigned Names and Numbers) definition of "end-users": technical, research, academic, government, end-users and civil society.

This issue will be critical in the discussion of privacy versus security, an area where tension remains today. Norms of behavior are needed.

The role of IEEE? Provide "science diplomats." This concept emerged during the Cold War when American and Soviet nuclear scientists met to build bridges upon which the two nations' diplomats could meet. With its international foundation – chapters in nearly every country – the IEEE is uniquely positioned to create and support science diplomats.

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

Discussion focused primarily on the balance between security and privacy. This involved topics such as Internet of Things, surveillance, tracking, meta-data, MAC (media access control) addresses for privacy and others.

The tensions between actors are particularly strong between end-users and their desire for privacy and control and the interests of commercial entities, regulators and law enforcement. In terms of regulation, finding a balance between incentives and regulations for enterprises is an important challenge. Making privacy more convenient is worth exploring.

The TOR (The Onion Router) browser allows one to use the Internet without being tracked, but purportedly anyone who downloads that software is being tracked to prevent nefarious uses.

Local regulations present a mosaic of rules pertaining to security. For instance, in Detroit (US), the police are not allowed to use data from private security cameras whereas in the United Kingdom they are allowed.

Individuals can choose to simply shut off their devices and, presumably those devices' tracking capabilities, but many enterprises expect employees to be present and available for contact – potentially defeating employees' or a corporation's privacy efforts. There is also the issue of when is off not actually virtually connected.

No international consistency exists on how the tension between privacy and security is handled. Even within a region – say, the European Union – great variations exist due to culture and context. Regardless of the strength of local regulations, the enforcement of those regulations varies. A technological solution for upholding a regulation may not be available.

Interoperability presents an attractive driver for action and, once accomplished, the conversation likely will turn to trust and its mechanisms.

Templates such as the Child Online Protection Act (COPA) – passed by the U.S. Congress in 1998, the law never took effect after more than a decade of court review – may provide a basis for understanding how regulations work and their effectiveness.

What can IEEE do? Perhaps constitute a rapidly engaged task force to address privacy issues. Bring research to greater visibility through its various, established channels. Target policymakers with educational seminars, webinars and other outreach efforts.

4. Fragmentation of the Internet due to local policies and how to avoid it

The Internet today is subject to fragmentation.

What are the key technology, policy and market issues that are in tension regarding this issue?

[One post-event caveat: Fragmentation may or may not have negative consequences, as fragmentation in how the Internet is governed, administered or used may simply reflect the prerogatives of sovereign governments. Whether fragmentation always has negative consequences or has potentially beneficial consequences should be further examined. If fragmentation is deemed negative, the benefits of a unified approach need articulation.]

Technology tends to be universal, policy local. However, technology may also fragment, driven by local preferences or mandates. Market issues such as net neutrality also follow different models that arise from local economics and business models. An Internet crime in one country may not be illegal in another country; some countries, e.g., have not outlawed child pornography. If data passes from one country through another en route to a third, e.g., each country is likely to have different data surveillance rules. Which country's rules, if any, should apply to that data?

Edge devices enabled by the Internet of things provide remote access points which may lead to a new understanding of cybersecurity and privacy.

Stakeholders include government, end users, multi-national enterprises, yet international consistency is lacking.

IEEE role? Possibilities include an ETAP-related effort to engage local policymakers. Perhaps government regulatory agencies could float their policy trial balloons and have them vetted by an international, politically neutral organization such as IEEE, which could provide feedback on the resulting consequences and trade-offs.

5. Algorithmic decision making that exacerbates existing power balances/ethics

An algorithmic function or an autonomous system may come to play the role of another team member in an operational setting.

In such a scenario, what are the key technology, policy and market factors and tensions that need to be considered? There's a general lack of understanding about how algorithms work. Code developers often eliminate ambiguities in software by making choices. Laws and regulations may be ambiguous; code is not. Cars today are legal to drive, but when they become automated, manual driving may become illegal. So technology and market factors (e.g., autonomous vehicles) may influence regulations, when in the past the reverse has often been true.

Can there be accountability for decisions made by algorithms? If so, where or with whom does it reside? And how do autonomous systems affect human behavior? With autonomous systems optimizing certain processes, how would, say, a doctor change the way he/she practices medicine?

Stakeholders include developers and writers of algorithms, data providers, users of the algorithms, including enterprises and consumers, and regulators, legislators and law enforcement.

The group found little if any international policy consistency in the domain of algorithms, but noted that in aviation, e.g., a significant level of consistency exists.

IEEE's role in this area could include providing insights into how algorithmic decision-making is developing and what directions it's likely to take in the future. IEEE could play the role of an unbiased evaluator of sources of data, possibly for standards development. IEEE could become a validator of algorithms or an evaluator of algorithm performance or a developer of testing methodologies for algorithms, especially in high-value use cases where lives may be at stake. Also, IEEE could develop testing standards, particularly in cases where regulators might require them.

6. How to best engage IEEE as a platform for contributing to the resolution of these and related issues

IEEE’s strength lies in its diversity. IEEE encompasses industry, academia, government, a vast array of domain expertise in technical disciplines, copious cross-domain activities and geographic diversity. This diversity needs to be leveraged.

Ethics, law and cultural factors involved in solving Internet governance challenges should no longer be declared “out of scope.” These and other formerly tangential elements need to be integrated into IEEE-related deliberations and affect outcomes.

Per tensions between technology, policy and the market: the market pushes for shortest time-to-market, technologists work methodically, collaboratively, but social and political actors involved in policy are missing. Another market element consists of end users who may not understand how changing technologies are changing the way they work. Maybe technology design needs to address how the world works, rather than how we’d like it to work.

Thus, perhaps initial moves towards a solution should include expanding the number of stakeholders involved in the process of Internet governance (adding social and political actors), expanding IEEE’s scope to integrate factors often formerly cited as being “out of scope,” and make more visible the role models for the technology-policy conversation so that aspiring engineers can visualize it. Failure analysis needs more attention in formal “lessons learned” case studies to improve best practices. Improve the ability to talk about the social implications of technology. Improve the ability to communicate with the intent to influence – a skill set that’s inadequately addressed.

All 20 issues identified at the inaugural ETAP meeting are articulated in Appendix II and may form the basis for future ETAP discussions, just as issues may be added as the ETAP Forum moves around the world.

Conclusion: Next Steps

This first ETAP identified 20 key issues, a list to which IEEE could contribute. From this list of twenty, six issues were classified as high priority.

The participants in this ETAP Forum also concluded it is of benefit to conduct additional ETAP forums around the word to obtain a global view. Additional ETAPs are being scheduled to fulfill this request. The best way to learn about a new ETAP event is to click on this IEEE website.

Each future ETAP will focus on and refine the six top issues identified, with the goal of moving several to a format for action. In addition, the open nature of the ETAP Forum is intended to allow regional participants to introduce priority issues of their own. The process of identifying the top issues around the word is thus iterative, and involves continuous discussion.

This discussion takes place in the IEEE Experts in Technology and Policy Online Community.

Appendix I:
List of ETAP I attendees and their affiliations

Andrews, Clinton, Rutgers University, ETAP Forum facilitator

Bennett, Richard, Visiting Fellow, American Enterprise Institute

Bhardwaj, Manu K., Senior Advisor, U.S. State Department's Office of Communications and Information Policy

Bielby, Jared, University of Alberta, ICIE

Brennan, Joan, Executive Director, Kantara Initiative, IEEE facilitator

Cam-Winget, Nancy, Distinguished Engineer, Cisco

Carson, Phil, writer, Thought Leadership Services, LLC, for Interprose PR

Chachich, Alan, U.S. Department of Transportation, Volpe, Nat'l Transportation Systems Center

Chandrasekaran, Sri, IEEE staff

Cioffi, John, ETAP Ad Hoc Committee, Department of Electrical Engineering, Stanford University

Clark-Fisher, Kathleen, Program Director, IEEE Cybersecurity Initiative

Cong Zhu, Julie, CNNIC

Day, Gordon, IEEE Ad Hoc Committee on Global Public Policy

De Souza, Evelyn, Cisco, Chair, Compliance & Data Privacy, Cloud Security Alliance Data Governance Working Group

Diamond, Stephen L., IEEE Computing Society, founder and Chair, IEEE Cloud Computing Initiative, IEEE Cloud Computing Standards Committee

Durand, Alain, Principal Technologist, ICANN

Evans, Jeffrey. Georgia Technology Research Institute, Director, Information and Communications Lab

Fonash, Peter, U.S. Department of Homeland Security, Chief Technology Officer, Cybersecurity and Communications Office

Grier, David Allan, IEEE Fellow, former President, IEEE Computer Society

Groopman, Jessica, analyst, Altimeter Group

Harkins, Daniel, Vice President, operations, Aruba Networks

Higa-Smith, Karyn, Program Manager, U.S. Department of Homeland Security

Karachalios, Konstantinos, Managing Director, IEEE-Standards Association,
ETAP Ad Hoc Committee

Katiti, Edmund, NEPAD e-Africa Programme

Lee, XiaoDong, CEO/CTO, China Internet Network Information Center. Professor, Chinese Academy of Sciences

Logvinov, Oleg, Director of Special Assignments, Industrial and Power Conversion Division, STMicroelectronics. Chair, IEEE Internet Initiative, Chair, IEEE P2413 "Standard for an Architectural Framework for the Internet of Things (IoT)," IEEE-Standards Association’s Corporate Advisory Group, ETAP Ad Hoc Committee

Loper, Margaret, Georgia Technology Research Institute, Information & Communications Lab

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

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

Northrop, Jeff, Chief Technology Officer, International Association of Privacy Professionals

Palmen, Cathy, president, Interprose PR

Rauscher, Karl, IEEE, MIT, Information security, consultant to ETAP process

Savage, James, IEEE USA

Savage, John E, Brown University professor of computer science, IEEE Fellow

Schulzrinne, Henning, Professor of computer science, electrical engineering, Columbia University, advisor to FCC

Shannon, Greg, Chief Scientist for the CERT® Division at Carnegie Mellon University's Software Engineering Institute, IEEE Senior Member

Slomovic, Anna, PhD., Lead Research Scientist, George Washington University, Cyber Security Research and Policy Institute, consultant to ETAP process

Tepper, Harold, Senior Program Director, IEEE, Avaya Communications

Tien, Lee, Senior Staff Attorney, Electronic Frontier Foundation, Adams Chair for Internet Rights

Tonti, Bill, PhD., EE, IEEE Senior Director

Ward-Callan, Mary, IEEE Managing Director, Technical Activities (since 1997),
ETAP Ad Hoc Committee

Wei, Joseph, Chair, Santa Clara Valley Section, IEEE

Wendorf, James, IEEE Internet Initiative Program Director

Wilkinson, Heather

Wong, Bobby, Future Directions Program Director, IEEE

Appendix II:
List of priority issues identified by participants in the inaugural ETAP Forum

1. Protecting Internet traffic and preventing meta-data analysis, yet link user location and Web address for law enforcement
2. Providing informed consent and tracking it through the information lifecycle
3. Opt-in versus opt-out from consumer standpoint
4. Feedback loop between advancing technology and unintended consequences, between technology and critical problems
5. Multi-stakeholderism: how can multi-stakeholder paradigm be established for technology/policy development. (No global understanding of “multi-stakeholder governance” yet it exists.)
6. Fragmentation of the Internet due to local policies and how to avoid it.
7. How can we have both security and privacy at scale/globally. Is there a policy component? Can a global policy be established, with derivatives for specific localities?
8. How can the integrity of the manufacturing process be ensured to produce secure products?
9. Data analytics, pro and con. Can data analytics be applied for security and privacy? Can data analytics serve anonymization at the “edge” of the network? Is it a potential threat if applied at intersection of cloud streams?
10. Potential risks and opportunities over integrating the Internet into traditional industries.
11. How best can IEEE serve as a platform for resolving issues as well as informing practicing engineers to build secure and privacy-respecting devices?
12. When do security and privacy compete, versus reinforcing each other? Can we develop criteria to encourage security and privacy to play well together?
13. Reconstructing institutions to better exploit and take responsibility for their actions.
14. Algorithmic decision making that may exacerbate existing power balances and ethical concerns. Hybrid teams (people and machines).
15. Who owns data when data is everywhere?
16. How should policy influence company data use and sharing?
17. How can we evolve the discussion of privacy to create tools for data manageability?
18. Resolving the benefits of our ability to handle big data versus protecting privacy. What are the trade-offs? The challenge of the anonymization of big data.
19. How can suspicious activity reports be shared legally and in a way that respects the privacy of users?
20. How do machines and people learn to trust one another, especially at scale? How can we have secure and trusted communications between devices? How should we define IHIT (In Hardware I Trust) in IoT? How do we identify misbehaving IoT devices?