



ITAC Newsletter N° 3 June 2014

June 19, 2014

Table of Contents

[From Seoul 2008 to Mexico 2016: On the Road to Cooperation and Economic Growth](#)

By Constance Bommelaer Senior Director, Global Policy Partnerships, and Nicolas Seidler, Policy Advisor, The Internet Society

[IPv6 and the Internet of Things](#)

By Vinton G Cerf, Vice President and Chief Internet Evangelist for Google

[Multistakeholder Partnerships for Economic Growth and Social Development](#)

By Kathy Brown, CEO & President, The Internet Society

[Review of the OECD Security Guidelines: An Update](#)

By Jane Hamilton, Senior Policy Advisor, Industry Canada, Chair, OECD WPSPDE

[Shifting from Identity Access Management to Identity Relationship Management: Drive Revenue Growth through Agility & Scalability of Trustworthy Tools](#)

By Joni Brennan, Executive Director, Kantara Initiative

[The Globalization of ICANN](#)

By Government Engagement Group, ICANN

[Capacity Building in the African Region](#)

By Adiel Akplogan, CEO, AFRINIC

[OECD Privacy Experts Round-table](#)

By Robin Wilton, Technical Outreach for Identity and Privacy, The Internet Society

[From Seoul 2008 to Mexico 2016: On the Road to Cooperation and Economic Growth](#)

June 19, 2014

Editorial by [Constance Bommelaer](#) Senior Director, Global Policy Partnerships, and [Nicolas Seidler](#), Policy Advisor, The Internet Society



Back in June 2008, the OECD Seoul Ministerial meeting articulated a collective vision of a future economy and society supported by the Internet. Significantly, this vision was to be sustained and strengthened by the concerted action of diverse stakeholders; not only governments and business - which were originally part of the OECD processes - but also civil society and the Internet technical community.

This meeting was a milestone in the development of Internet policy-shaping processes based on multistakeholder participation mechanisms. Back in 2008, Ángel Gurría, OECD's Secretary General, stated in his final remarks:

"A more decentralized networked approach to policy formulation for the Internet economy also includes the active participation of stakeholders. Such active participation needs to be the norm. (...) we need to go further. I would recommend that we begin the process of formalizing the participation of civil society and the technical community in the work of the OECD on the Internet economy."

This was truly visionary. Five years later, ITAC is a well-identified and respected Committee, gathering [28 organizations](#) from the Internet technical community. Its experts contribute to enlightening the work of governmental delegations from across 40 economies on critical issues such as [IPv6](#) , [security](#) and [capacity building in developing countries](#).

This spirit of collaboration is at the heart of the OECD Internet Policy Making Principles ([IPPs](#)), which recognize “the reliance of our economies on the Internet, the global nature of the Internet, and the various approaches implemented to stimulate the Internet economy, including innovative governance strategies in convening diverse groups of stakeholders to forge consensus (...).”

Over the past five years, the impact of the Internet on the economy has accelerated, while the underlying foundations and value of cooperation among all stakeholders have remained. This multistakeholder approach will be essential as we tackle new challenges, whether in the areas of security, risks related to personal data, or the development of an effective and interoperable global network access.

An encompassing approach that underlines the economic and social benefits of an open Internet will be essential as we march together from Seoul 2008 to Mexico 2016, on the road to cooperation and economic growth.

[IPv6 and the Internet of Things](#)

June 19, 2014

By Vint Cerf, Internet Pioneer



William Gibson is reported to have said: **“The future is already here — it’s just not very evenly distributed.”** Whether this is an accurate quote or not, it captures precisely what we are (slowly) facing as IPv6 moves from its 15 year slumber from about 1996 to the June 6, 2011 world IPv6 day when many operators of Internet services turned on IPv6 for a day. It was turned on, again, permanently on June 6, 2012. Two years since that time, one is beginning to see growth in the use of this important protocol in support of an expanded address space.

Why is this important? For one thing, we are starting to see more and more devices and appliances outfitted with Internet Protocol capability (“Internet-enabling”). It is entirely conceivable that many billions of devices, from light bulbs to industrial equipment, will become a part of the vast Internet fabric. Interconnection and interoperability open an endless frontier for new applications and services. They also open up new avenues for serious abuse. For anyone working on new applications that rely on Internet-enabled devices, security, authenticity, access control and the like will be fundamental to successful deployment.

The ability to configure many devices to accept control or to supply reports only to authorized parties is part of the challenge. When you bring a new, Internet-enabled device(s) into an already enabled environment, it must be possible to add the new device(s) without accidentally adding your neighbors’ devices by mistake. Making this process seamless, secure and intuitive is not going to be a simple matter and demands serious design attention.

Perhaps there are some lessons one can take from Bluetooth experiences although this process seems to work best for pairing of devices for peer-to-peer operation. Society stands to benefit from the resulting smart homes, smart cities, smart cars and smart personal devices, if we can get the framework right. Gathering health

indicators on a continuous basis may allow prompt diagnosis of serious conditions, for example. Tracking traffic may allow cities to manage traffic flow and monitor resource usage to avoid brownouts or other resource shortages.

I am convinced that devices such as Google Glass, among others, may open the door to a number of beneficial applications in which local and remote computers can be used to process sensor information, produce augmented reality effects, and help us react in near real time to changes in our immediate environment. One can already see early efforts to achieve real-time translation of spoken languages, translation of text documents viewed through a mobile lens, and speech synthesis to guide visually impaired users to new destinations.

Sometimes, I wish I were 8 years old so I could see what the world will be like in the 22nd Century!

Vint Cerf is an American internet pioneer, who is recognized as one of “the fathers of the Internet”, sharing this title with American engineer Bob Kahn. His contributions have been acknowledged and lauded, repeatedly, with honorary degrees and awards that include the National Medal of Technology, the Turing Award, the Presidential Medal of Freedom, and membership in the National Academy of Engineering.

[Read More:](#)

[Multistakeholder Partnerships for Economic Growth and Social Development](#)

June 19, 2014

By [Kathy Brown](#), CEO & President, The Internet Society



We are in the midst of a very busy global policy dialogue on Internet governance and, in fact, 2014 could be an inflection point in shaping the future of the Internet and its governance. In an increasingly complex environment, stakeholders are seeking global guidelines and frameworks to address a wide range of local requirements.

The Internet is set to pass 3 billion users early next year, and while the open Internet is an unparalleled positive force for economic and social progress, it is not immune from economic and political influences that can limit its benefits. Many of the benefits, and challenges of delivering the Internet to everyone and for everyone are highlighted in the [Internet Society's Global Internet Report](#).

This report highlights why we must not lose sight of how the Internet, based on the principle of openness — open technical standards, open to everyone, open for innovation, and open multistakeholder governance — has transformed societies and empowered people all around the world. We must also not take these principles for granted.

As the Internet governance dialogue evolves, we must remember that we already have proven principles to show us the way. In particular, the inclusion of all stakeholders as participants in the Internet's evolution is essential. Experience shows that bringing together stakeholders from different perspectives can produce sound and thoughtful policies. In this regard, the 2008 OECD Ministerial was a landmark in opening doors for the technical community to provide its expertise on Internet policy issues. Today, the Internet Technical Advisory Committee ([ITAC](#)) gathers nearly 30 organizations from the technical community, coordinated by The Internet Society, who have developed strong and trust-based working relationships with the OECD community.

Since the adoption of the OECD Internet Policy Making Principles (IPPs) in 2011, consensus building among different stakeholders has constantly progressed. Many of these principles have shown their relevance at the recent NETmundial in Sao Paulo. As I mentioned in [my post NETmundial blog](#), this conference demonstrated transparency, meaningful participation of all stakeholders, and true consensus-building, which are at the heart of the multistakeholder process. It gave us a renewed appreciation for what a multistakeholder approach could produce.

The OECD IPPs remain critical as we work towards the next OECD Ministerial conference. A key challenge is to go beyond affirmation and build upon these principles towards concrete action and common understanding. And we need to do that together, among stakeholders with diverse expertise, interests, and from different regions. Sharing both best practices and difficulties in the application of these principles is essential in view of a stocktaking exercise at the 2016 OECD Ministerial.

As we head towards the next key events on the Internet governance agenda - including the 9th Internet Governance Forum in September 2014 - let's concentrate on how all stakeholders (governments, technical organizations, private enterprise, civil society, and others) can better work together to tackle challenges. There may not be a one-size-fits-all multistakeholder model that is identical from region to region or from one institution to the other, but all multistakeholder approaches should be linked by common principles of openness, inclusiveness, and transparency. This is the only path to realizing our shared goal of an open and secure Internet for all.

[Review of the OECD Security Guidelines: An Update](#)

June 19, 2014

By Jane Hamilton, Senior Policy Advisor, Industry Canada, Chair, OECD Working Party on Security and Privacy in the Digital Economy



In 2013, the Working Party on Security and Privacy in the Digital Economy Information Security and Privacy[1] launched its review of the 2002 OECD Guidelines for the Security of Information Systems and Networks by organizing an informal multistakeholder consultation of experts from its membership and beyond, to facilitate a discussion of the need for revisions to the Guidelines. The scope of the discussion was broad and ambitious. We explored how the core security principles should be modernized, identified what recommendations the OECD should make to governments, and shared ideas on how international co-operation should be addressed.

Over the course of 12 months, more than 100 experts with a diverse range of perspectives discussed six working papers through exchanges in physical meetings, electronic discussions and by written contributions. The participation of non-governmental stakeholders representing the Internet technical community, civil society and business proved instrumental in the collection of key input to feed the reflection on this complex subject matter. As Chair of the Working Party, I am extremely grateful for the commitment of all to this work. Under the active leadership of ITAC, the debates spilled over into other fora such as the February WSIS+10 meeting hosted at UNESCO in Paris and the October 2013 Internet Governance Forum (IGF) held in Indonesia, with fruitful discussions under the thought-provoking theme “Cybersecurity: Throwing out pre-conceptions”.

These vibrant discussions led to agreement in December 2013 that the Guidelines should be revised. A new and more formal process has now begun, with the aim of reaching a consensus among all Working Party delegations, including those

representing non-governmental stakeholders, on the extent and specific nature of the revisions.

Awareness raising about “security of information systems and networks” was the primary objective of the OECD in 2002. However, as security incidents are making the headlines more and more, today’s OECD priority is to help government public policy makers and decision makers in public and private organizations to understand cybersecurity as the management of economic and social risks associated with the use of ICTs and the Internet to realize economic and social benefits. The participation of all stakeholders in contributing to the thinking and shaping of the consensus, as well as promoting the OECD’s final messages after the adoption of the revised Guidelines, is essential.

As Chair of the Working Party, I look forward to the continued active participation of ITAC in this very important work and the expertise and informed perspectives its members bring to the discussions. I am particularly appreciative of the contributions made by Christine Runnegar and her team during our very lively meeting debates.

[1] Formerly known as the Working Party on Information Security and Privacy (WPISP).

Jane Hamilton has been working with the Canadian federal government since 1998. In her current capacity as Senior Policy Advisor with Industry Canada’s Digital Policy Branch, Jane’s focus is on policy development related to building trust and confidence in the digital economy. This work involves both security and privacy aspects.

Prior to working with the federal government, Jane worked for over 12 years in the financial services industry. As a member of the senior management team of the Canadian Payments Association, Jane was responsible for the development of policies and standards for new forms of electronic payment. Jane assumed the role of Chair of the OECD’s Working Party on Security and Privacy in the Digital Economy in 2011.

[Shifting from Identity Access Management to Identity Relationship Management Drive Revenue Growth through Agility & Scalability of Trustworthy Tools](#)

June 19, 2014

By Joni Brennan, Executive Director, Kantara Initiative



Introduction:

In the interest of supporting trust toward economic growth, the OECD Privacy Guidelines provide a tool for privacy best practices supporting European Union data protection legislation (and cultural expectations) as well appropriate transborder flow of personal data. The IEEE-SA and Kantara Initiative provide this article as participating members of the OECD-ITAC to discuss the changing nature of identity management with more focus toward relationships between people, entities, services, and things. The concepts provided are observations in development within the Kantara Initiative open and transparent community.

Identity and access management (IAM) is the security discipline that enables the right individuals to access the right resources at the right times for the right reasons [1]. IAM services were traditionally built for a company's internal use, to assist with manual on and off boarding and for establishing access privileges to organizational data and systems. Today organizations must implement a dynamic IAM solution that serves employees and customers, partners and devices, and all those in between, regardless of location. This is the evolution of IAM to Identity Relationship Management (IRM).

IRM evolves IAM by focusing on:

- business values of consumers and things, adaptability, top line revenue, and velocity.
- technical values of internet scale, dynamic intelligence, borderless, and modular.

As people and “things” are assigned identities across networks simple, flexible and scalable IRM services designed to quickly verify identities and access privileges become imperative for any business or institution to safely and efficiently engage with their users. People expect solutions to link devices from laptops to social apps into a single secure platform that works anywhere at anytime. Basic trust of stakeholders in these ‘shared spaces’ is key to enabling market growth and innovations.

With more networked devices sharing data, privacy tools are paramount to ensure systems are trustworthy. References are made to “contextual identity”, where “context” focuses on connectivity and data that reveals something about a user. Use of context can improve the user authentication experience. However, enabling use of personal data while protecting users’ privacy is challenging. Communities must understand how this data may be used and what governance policies are necessary. Communities must provide user data control tools to enable trust. Examples include Privacy Lens [2], an Internet2 pilot funded by the US National Strategy for Trusted Identities in Cyberspace, and User Managed Access (UMA) [3] for resource authorization, a project of Kantara Initiative. Vendors may review the OECD Privacy Principles [4] for a sense of their performance regarding respect for user privacy.

Conclusion:

We suggest organizations engaging with hyper-connected customers to:

- Understand the risks your organization takes in context of the resources used to manage current and future systems for customer and vendor relations.
- Limit data collection to only what is needed to safely perform a transaction.
- Be transparent about your data collection and practices
- Connect with your peers and competitors through vendor neutral consortia.
- Seek solutions that have been verified by a neutral body.
- Adopt industry standards and build your unique optimizations around them.
- Adopt third party vendors who deploy open standards.

When shifting from the closed world of IAM to the open world of IRM, advanced user engagement tools are necessary to protect privacy while providing dynamic engagement.

Source:

[1] <http://www.gartner.com/it-glossary/identity-and-access-management-iam/>

[2] <https://spaces.internet2.edu/x/RILYAg>

[3] <https://kantarainitiative.org/confluence/x/LgAPAQ>

[4] <http://oecdprivacy.org>

Joni Brennan builds diplomatic and collaborative relationships within and across communities of interest. She participates in international organizations and industry standards committees including: OECD ITAC, ISOC, IEEE, OASIS SSTC, ISO SC27 WG5, and ITU-T SG17 Q6. She has served as the NSTIC / IDESG Trust Framework WG

Chair. She has provided testimony regarding Trusted Identity and Access Management systems for the US ONC HITSP as well. Joni has helped drive and formalize strategic partnerships between Kantara Initiative and organizations including: Geant, Terena, OASIS, IDESG, DirectTrust and EHNAC.

She leads Kantara Initiative as the premiere Trust Framework Provider facing multiple industry sectors. As a US ICAM Trust Framework Provider Kantara Initiative will provide Accreditation and Approval verifications for Identity Providers / Credential Service Providers to be deemed qualified for access to connect to the US Federal Cloud Credential Exchange. In addition, working with multi-stakeholder representation, Joni has help to ensure that the Kantara Initiative program is aligned and referenced in multiple eGovernment strategies including: Government of Canada, New Zealand, and Sweden.

Joni has over a decade of service to the IEEE Standards Association (SA) and Industry Standards and Technology Organization (IEEE-ISTO) as a Senior Program Manager . She is a member in good standing of the American Society for Association Executives (ASAE) and an honors graduate of of the first class of Rutgers University Information Technology and Informatics (ITI) programme at the School of Communication and Information (SC&I).

The Globalization Of ICANN

June 19, 2014

By: Government Engagement Group, ICANN



The Internet Corporation for Assigned Names and Numbers (ICANN) was formed in 1998. Then there were about 150 million global Internet users, and only 7 Generic Top Level Domains (gTLDs). Today there are more than 3 billion Internet users, with at least 300 gTLDs (many of them offering names in non-Latin scripts) by the end of 2014.

Since its foundation, ICANN's mission has always been global in context. With an international Board (with mandated representation from each Region) and a Community with business, civil society, users and government representatives from across the globe actively engaged in every aspect of ICANN's work.

Under the leadership of the President and CEO Fadi Chehade, the program has been significantly intensified, with the establishment of three operational Hub Offices in Singapore, Istanbul and Los Angeles, as well as the opening of engagement offices in Beijing, Geneva, Montevideo and Seoul.

This approach, along with a corresponding recruitment of additional staff into the Global Stakeholder Engagement (GSE) team, has witnessed a significant growth in participation of all stakeholders in ICANN meetings, as well as participation of ICANN in discussions related to Internet Governance.

In March 2014, a further significant step on the globalization agenda took place, namely the US DOC announcement on their intended transition of the stewardship of the IANA functions to the global multistakeholder community. ICANN was asked to initiate a global dialogue on a multistakeholder mechanism to replace the US

government's stewardship role. To join the discussion, and contribute with ideas go to: <http://www.icann.org/en/about/agreements/iana/transition>
The globalization of ICANN is taking place against the backdrop of a global discussion on Internet Governance that the OECD has and will play an important role in (not least in the run up to the 2016 Ministerial).

With the adoption of multi-stakeholder OECD Internet Governance Principles in Paris in 2011, the ITU's WCIT in 2012, the Brazilian hosted NetMundial Conference in April this year and the Report in May from the High Level IG Panel, a lively debate and discussions is taking place on the need for improving the current Ecosystem on Internet governance that might enhance the ability of it serve the needs of all stakeholders.

ICANN, both in the ITAC at OECD (which we find an excellent fora), and with other stakeholders, among them the Internet Engineering Task Force (IETF), the Internet Society (ISOC), and the World Wide Web Consortium (W3C); have been privileged to have been involved in these debates.

These discussions will continue through 2014 and beyond. The IGF is to take place in September in Istanbul; the ITU will have its Plenipotentiary Conference (PP-14) in Busan, South Korea in October and the UNGA looks set to discuss the Review of the World Summit on Information Society (WSIS) in 2015.

The multi-stakeholder approach for development of policies with respect to the governance of the Internet is thus dynamic and vibrant, but also faced by many challenges. We, however, believe that keeping, and further developing, the Internet as an open, interoperable, and innovative force for development and growth, governed in a bottom-up and inclusive way, and accessible for all, is a goal worth striving for.

ICANN is a not-for-profit public-benefit corporation with participants from all over the world dedicated to keeping the Internet secure, stable and interoperable. It promotes competition and develops policy on the Internet's unique identifiers. Through its coordination role of the Internet's naming system, it does have an important impact on the expansion and evolution of the Internet.

Capacity Building in the African Region

June 19, 2014

By Adiel Akplogan, CEO, AFRINIC



The African Network Information Centre (AFRINIC) is the Regional Internet Registry (RIR) for Africa and the Indian Ocean region. Aside from distributing IPv4, IPv6 and Autonomous System Numbers (ASNs) to 56 economies in its service region, AFRINIC plays a leading role in capacity building initiatives, including technical training, supporting infrastructure and technology development, community outreach and engagement activities.

This article highlights the importance of developing local infrastructure and capacity building in order to support the development of local content, e-commerce and ultimately economic progress and social development.

Internet penetration in Africa has grown by more than 100% over the past three years and now stands at around 15%. This increase is mainly due to the development of fibre connectivity around and within the continent. It's also estimated that Africa has the highest level of Internet penetration growth through mobile devices in the world, with the region having around 650 million mobile phone subscribers.

Developments are moving relatively fast throughout AFRINIC's region. To improve the efficiency of Internet bandwidth usage and the overall stability of Internet infrastructure, AFRINIC supports various projects including the deployment of anycast root server copies. So far, three countries have deployed root servers directly through AFRINIC's root server copy project (AfRSCP). There are currently 19 root server copies in Africa, five of them co-funded by AFRINIC, with five more copies currently planned for deployment in the region.

AFRINIC also offers its own Anycast DNS service for African ccTLDs, providing a secondary service to IANA for IPv6 reverse zone (e.ip6.arpa), and actively supports the setup of local and regional Internet Exchange Points (IXPs) throughout Africa as

part of the AXIS project, helping to keep traffic local and lowering transit costs for the region.

An important part of AFRINIC's capacity building efforts are focused on facilitating education and knowledge-share with free training courses delivered throughout Africa as well as online. The learn.afrinic.net initiative offers training on IPv6 deployment, Internet number resource management, DNSSEC and RPKI to network engineers and non-technical participants. Since 2004, over 90 training sessions have been given with more than 2,000 individuals receiving free training.

It is critical for the African and global Internet that the African continent's networks are scalable, resilient and IPv6- ready to ensure reliable and open access for the millions of future Internet users in Africa and to facilitate technological innovation aimed at solving the region's unique issues. AFRINIC's contribution to Internet infrastructure projects impacts the development of local infrastructure, content development and e-commerce, enabling local communities to benefit from the global e-economy and ultimately leading to economic progress and social development in the African region.

More about AFRINIC:

www.afrinic.net

More about AFRINIC's root server copy project:

<https://www.afrinic.net/en/initiatives/root-server-copy>

AFRINIC's Training Website:

www.learn.afrinic.net

More about the AXIS project:

<http://www.internetsociety.org/events/workshops/axis-project-and-axis-workshops>

Adiel A. Akplogan is the Chief Executive Officer of AFRINIC Ltd., the Internet Numbers' Resource Registry for Africa since 2004. With more than 15 years experience in the Internet Industry, he has previously worked as New Technology Director at CAFENet (an IT service company based in Togo - 1994-2000), then as Information System Manager of Symbol Technologies in France (2001-2003).

He has served as member of the UN Secretary General Internet Governance Forum Advisors Group (IGF-MAG from 2006-2009), in the African Technical Advisory Committee of the United Nation Economic Commission for Africa (ATAC/UNECA from 2005-2006) and in the OIF (Organisation Internationale de la Francophonie) group of Expert on Internet Governance since 1999.

As CEO of AFRINIC, Mr. Akplogan has served as the Chair of the NRO Executive Council in 2009 (Number Resource Organization - www.nro.net) and was involved with the setting up of several technical coordination bodies in Africa such as the African Network Operators Group (AfNOG) where he serves as a member of the Administrative committee and the African ccTLD Managers Association (AfTLD).

Adiel is an Electrical Engineer and holds a M.Sc. in E-Business and New Technology Management.

[OECD Privacy Experts Round-table](#)

June 19, 2014

By [Robin Wilton](#), Technical Outreach for Identity and Privacy, The Internet Society



Subject Access Requests

What is the data controller's perspective on subject access requests (SARs)? The bottom line is that, for data controllers, responding to subject access requests requires preparation, investment and effort.

Finding the right data to respond can be non-trivial; application silos, missing metadata/keywords/indexing, constantly-increasing volumes of data: all increase the cost of servicing SARs. Data may need redaction for 3rd party names or confidential information; this requires subjective judgement.

These factors make SAR responses increasingly hard to automate without raising the risk of privacy and compliance problems.

Three themes to address

First: the shift from identifiers to 'big data' and attributes. Traditionally, identity is "what you get by being issued with a credential by a trusted source". The "modern" model of identity is "what can be inferred from attributes and metadata", even if those come from less trusted sources.

Linkability in large datasets depends less and less on "traditional" identifiers, and more on attribute and inference data.

Second: "friction" in online service provision. Service providers make it easy to sign up, but hard to unsubscribe. Even if a user unsubscribes, service providers may retain data about that user.

There's no financial incentive for service providers to encourage disengagement; the benefit of retaining user data is considered to outweigh the potential cost of remaining responsible as a data controller.

Third: monetization of personal data is a complex ecosystem with several “food chains”, mostly invisible to the user. With each step, users' awareness of and ability to control data about them decreases, with corresponding privacy risk.

Conclusions

Users have little ability to control what is done with data that has an actual or potential impact on them. With big data, the impact on an individual's privacy and self-determination is increasingly likely to originate in data about others, and inferences drawn from it.

It is no longer necessary for you to display a pattern of consumer behaviour, provided you reveal some piece of data which places you in a particular consumer category. The behaviour of others is enough to produce an impact on you. If we only consider subject access to those entities the data subject knows about, we will miss many of the cases that result in privacy impact on the individual.

How to Become a Member

ITAC provides an avenue for new technical insights to contribute to the work of the OECD. ITAC is open to any Internet technical and research organization that meets the membership criteria listed in the Committee's Charter.

ITAC encourages Policymakers, members of Civil Society and Businesses to submit queries regarding any of our work to Questions@internetac.org

If your organization is interested in joining ITAC and contributing with technically informed advice to the OECD's development of Internet-related policies, we invite you to visit our website: internetac.org, to read the “Criteria for Membership” in ITAC's Charter (Section III).

For further Information on ITAC, please contact us at Membership@internetac.org