Internet Governance Forum 2016 Workshop #111
Session Title: Empowering and educating the next billion Internet Users

Date: December 6, 2016
Time: 9:00am PST
Session Organizer: Digital Citizens Alliance
Chair/Moderator: Dan Palumbo
Rapporteur/Notetaker: Shane Tews

List of Speakers and their institutional affiliations:
Shane Tews, American Enterprise Institute, Alexa Raad, Entrepreneurial Tech Executive and patent holder, James Ting-Edward, Issue Advisor at Internet NZ, Scott McCormick, President of Kvant Corp cyber security firm, Nilmini Rubin, Global Public Policy director at Tetra Tech

Key Issues raised (1 sentence per issue):
- Malware on mobile
- Cyber trust and Data collection
- Enabling Trust

If there were presentations during the session, please provide a 1-paragraph summary for each Presentation:

Please describe the Discussions that took place during the workshop session: (3 paragraphs)

The continued growth of the digital economy and the devices that support this infrastructure call for a more effective security capacity building structure as the expansion to the next billion users is created. Security and privacy of the shared data is a key concern for the next billion Internet users. Can we learn the lessons of the first billion users to create principles on how we should proceed?

The Mobile web is the most used element of the next generation Internet infrastructure. Can we co-design capabilities into the mobile web that have initiatives in mind for user readiness and security in mind? These were two key questions posed by the workshop participants.

Machine learning, physical presence of a device can help create a trust model using a collaborative architecture platform can be designed with predictive algorithms we know about mobile users; past behavior, normal usage including purchase pattern, can help make apps smarter using reputational norms and allowing a user to be protected from end-user scams that steal end-user data and potentially funds from the user of the mobile device.

Data privacy is also a major concern for current and upcoming technology. Mobile device apps privacy and user notices criticized for their difficult terms of use legal language and length of the legal notice that is not user friendly to the mobile device user. It was also noted the terms of service are difficult to translate in both the nuances of the terms of reference and the actual meanings into different languages from the original English source.

Recognizing the amount of data that is created and the immense amount of information that is available on the population by the default action of most user accepting the terms of use without understanding who then owns the data highlighted the question of who do you trust? And how do you know that the company is protecting the data that is shared?
How much information is actually sent out across the network when you use a mobile device? Access to your camera, access to your microphone, access to your contacts are all common requests of an app platform that have only a full agree to terms of use and not a per use capability. An example of sharing economy apps and their interest in keeping the app on to collect data on the user after the transaction had taken place highlighted concern over the lack of ability of the end user to authorize for a specific purpose for the benefit of the user and not a blanket invasion into the user’s behavior for the app owners use to sell the data to the market.

The Internet of Things (IoT) has great advantages for items connected to the Internet and to each other to allow interaction between devices and for remote command of a device. The lack of ability to manage basic security measures was a concern. The low cost for the device to make it more affordable is usually due to inexpensive components that is commonly paired with static passwords that cannot be changed to enhance security of the device. Open wifi capability the data running across the device easy to intercept and monitor is a continuing concern too. There is also very limited if any way to upgrade the software on the device due to the inexpensive design. These devices could be enhanced allowing other technology to inform on when and how the device should be able to be accessed. An example would be data or the Internet Protocol number as a geo-location device to cabin off who can access the controls to the IoT system. Many items could be programmed to ensure the person controlling the device is in the immediate vicinity to have access to the system lowering security concerns for use of IoT devices to enhance productivity and avoiding cyber concerns.

Creating, consuming and maintaining trusted applications is a goal for this group going forward. Creating pattern mapping, enhancing the expectation of management of an individual’s privacy when using technology and what context the information would be used as a way to control information that is gathered while using a mobile device.

The lack of support of a full digital economic integration was noted by a participant who used the recent demonetization of the two largest Indian currency notes as a mechanism to move the country to digital currency exchange through mobile technology. It was noted that while this is a laudable goal the country’s infrastructure was not ready for such a move due to the lack of infrastructure in most of the areas outside the key urban cities in India and 95% of the Indian population using cash for goods and services. The creation of a strong financial backbone to support moving the Indian economy to a digitally driven economy is not in place for this abrupt change. E-wallet providers are just getting in place in stalls at major shopping areas for help bring more citizens onto the mobile web payment platforms. This was noted as a lesson to be learned to move forward into the more rural areas for the next billion users.

It was noted in contrast to the Indian culture being caught unprepared for such an abrupt change to a digital economic bone the Chinese application “WeChat” is more of a portal and platform that is where the future should be headed. WeChat has created an app-within an app environment that creates credentials throughout the entire WeChat ecosystem has a smartphone penetration of 62% and this app that started as a social portal to send text, voice, and photos has used as a banking portal, taxi hailing, food ordering, fitness tracker, appointment booking, utility monitoring, news source all in one place that interacts amongst the capabilities. The apps ability to access utility bills and credit card statements acts as an unofficial verification on the user. The usage of the app continues to inform the platform to be able to access geo-located information such as city services.

WeChat is a mobile first approach to platform creation in China. It has become so popular that it’s application platform is being integrated into physical presence process payments, vending machines, restaurants, and hotels. The built-in trust validator through vetted partners offers a seamless experience for the end user. The more people who use the
The smarter the entire ecosystem becomes on user habits and ways to enhance the both the use and potentially protection of data.

Using the power of the Multi-stakeholder partnerships we can achieve a more secure and sustainable digital economy outcome. By working together, we can enable positive impacts in core emerging digital economy tools and infrastructure. We can improve information and technical development capabilities to the next billion users. Being aware of the dangers to end users while encouraging the growth of technology is an important goal to ensure sustainable development. We must monitor for both enhanced and secure outcomes that have a mutual understanding built in; that the safety of the end user has to be a priority while building out the future of the Internet.

Please describe any Participant suggestions regarding the way forward/ potential next steps /key takeaways:

All of these engagement opportunities unlock more information that have the potential for good uses for both the end users and the affiliated user of the valued and vetted application platform. We want to take the lessons learned that are positive for the consumers from these examples while being cognizant of the potential government access and obstruction in the data shared by these applications.

As we manage the continued tremendous growth of the capabilities and potential reach of these technologies to the next billion users we want to carry forward the lessons that will enable more security for the end user while enabling technologies that will enhance the platforms for innovation and creative opportunity.