the Internet is for everyone

Security and Privacy Issues in IoT Applications

Shernon Osepa

Manager Regional Affairs Latin America & the Caribbean

CANTO 32nd Annual Conference & Trade Exhibition

San Juan, Puerto Rico USA

3 August 2016

Internet Society

InternetSociety.org

Agenda

- Security themes
- IoT Overview: concepts and drivers
- Questions

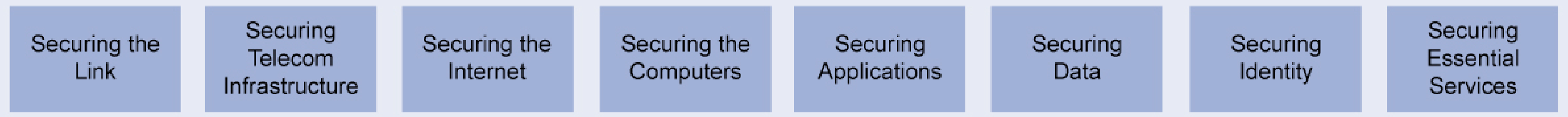
Definition of cyber security

- *“Cyber security refers to preventative methods to protect information from being stolen, compromised or attacked in some other way”;*

- Not every crime that occurs on the Internet is covered by the term cyber security. A **crime is a crime**, and simply moving it to the Internet doesn’t make it special!

Cyber Security Themes

- Because the scope of cybersecurity is so broad, it is helpful to break it down into these categories

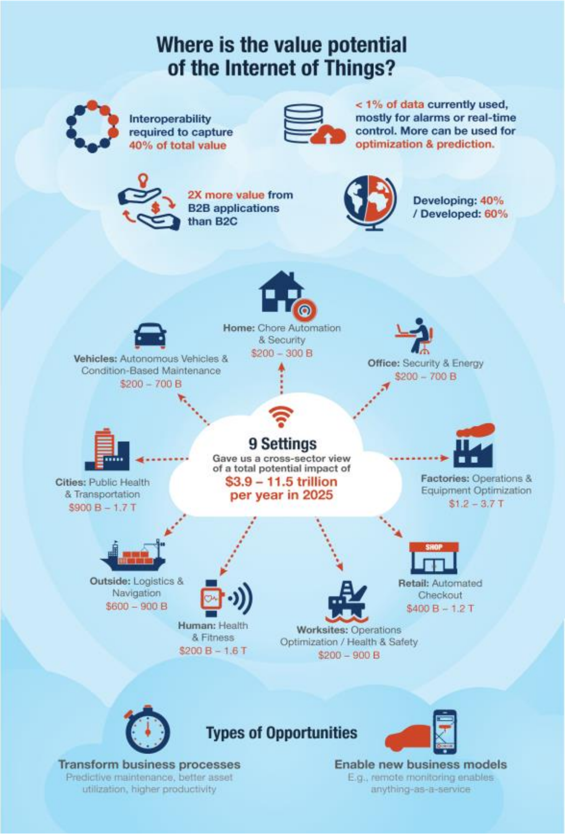


Cybersecurity Themes

IoT Overview: Concepts and Drivers

What is IoT really?

One view, from McKinsey Global Institute:


Where is the value potential of the Internet of Things?
Interoperability required to capture 40% of total value
< 1% of data currently used, mostly for alarms or real-time control. More can be used for optimization & prediction.
2X more value from B2B applications than B2C
Developing: 40% / Developed: 60%
Home: Chore Automation & Security $200 – 300 B
Vehicles: Autonomous Vehicles & Condition-Based Maintenance $200 – 700 B
Office: Security & Energy $200 – 700 B
9 Settings
Gave us a cross-sector view of a total potential impact of $3.9 – 11.5 trillion per year in 2025
Cities: Public Health & Transportation $900 B – 1.7 T
Factories: Operations & Equipment Optimization $1.2 – 3.7 T
Outside: Logistics & Navigation $600 – 900 B
Retail: Automated Checkout $400 B – 1.2 T
SHOP
Human: Health & Fitness $200 B – 1.6 T
Worksites: Operations Optimization / Health & Safety $200 – 900 B
Types of Opportunities
Transform business processes
Predictive maintenance, better asset utilization, higher productivity
Enable new business models
E.g., remote monitoring enables anything-as-a-service

- <u>**Despite the buzz, no single definition!**</u>

refers to scenarios where network connectivity and computing capability extends to objects, sensors and everyday items not normally considered computers, allowing these devices to generate, exchange and consume data with minimal human intervention.

- **Functionally:** The extension of network connectivity and computing capability to a variety of objects, devices, sensors and everyday items allowing them to generate/exchange data, often with remote with data analytic/management capabilities.

- **As Value**: *<u>Data</u>* & what can be done with it.

- **As a Vision**: The realization of a ‘hyper-connected” world.
  - This is why it matters.
  - This is why it’s hard.

Computers, Networks, and “Things”

“Machine to Machine” (M2M)
(~1970s +)

Internet of Things Beginnings

Carnegie Mellon Internet
Coke Machine (1982, 1990)

Trojan Room
Coffee Pot
(first webcam)
(1991)

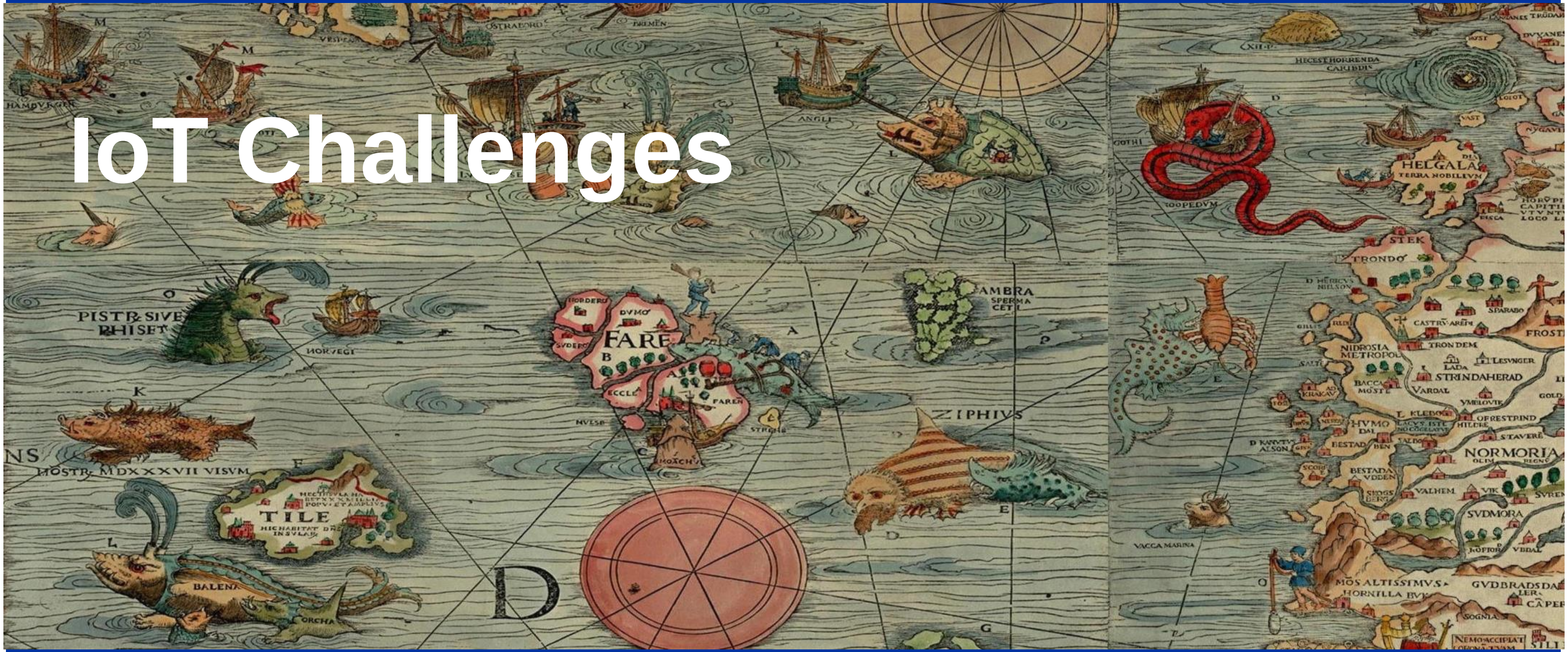
Internet Toaster
(1990)

If it’s not new, why now?:

A Confluence of Market Trends

- UBIQUITOUS CONNECTIVITY
- COMPUTING ECONOMICS
- ADVANCES IN DATA ANALYTICS
- WIDESPREAD ADOPTION OF IP
- MINIATURIZATION
- RISE OF CLOUD COMPUTING

IoT Challenges



Internet Society

US San Francisco Bay Area Chapter

Key IoT Challenges

- SECURITY
- PRIVACY
- INTEROPERABILITY AND STANDARDS
- LEGAL, REGULATORY AND RIGHTS
- EMERGING ECONOMIES AND DEVELOPMENT

Security

Security Must be a Fundamental Priority

- Security is the most pressing and important IoT challenge for industry, users, and the Internet.
- Growth in devices increases the surface available for cyberattack
- Poorly secured devices affect the security of the Internet and other devices *globally*, not just *locally*.

Developers and users of IoT devices and systems have a collective obligation to ensure they do not expose others and the Internet itself to potential harm.

A Spectrum of Unique Smart Object Security Challenges

- Cost/Size/Functionality
- Volume of Identical Devices
- Deployment at Mass Scale
- Long Service Life
- No / Limited Upgradability
- Limited Visibility into Internal Workings
- Embedded Devices
- Physical Security Vulnerabilities
- Unintended Use & BYOIoT

See also IETF RFC 7452 *Architectural Considerations in Smart Object Networking*

Collaborative Security Approach:

Developing Solutions in the Context of Principles

Fostering Confidence / Protecting Opportunities	*Opportunities* for individuals, business, economy and and society will only be realized if there is *confidence* in the Internet, systems, and technologies (including IoT).
Collective Responsibility	No security threats or solutions exist in isolation. Requires collective responsibility, a common understanding of problems, shared solutions, common benefits, and open communication channels.
Uphold Fundamental Properties and Values	Security solutions should be fully integrated with the important objectives of preserving the fundamental properties of the Internet and fundamental rights.
Evolution and Consensus	Security solutions need to be flexible enough to evolve over time & responsive to new challenges. Focus needed on defining agreed problems and finding solutions, including incremental ones.
Think Globally, Act Locally	Creating security and trust requires different players (within their respective roles / responsibilities) to take action and close to where the issues are occurring.

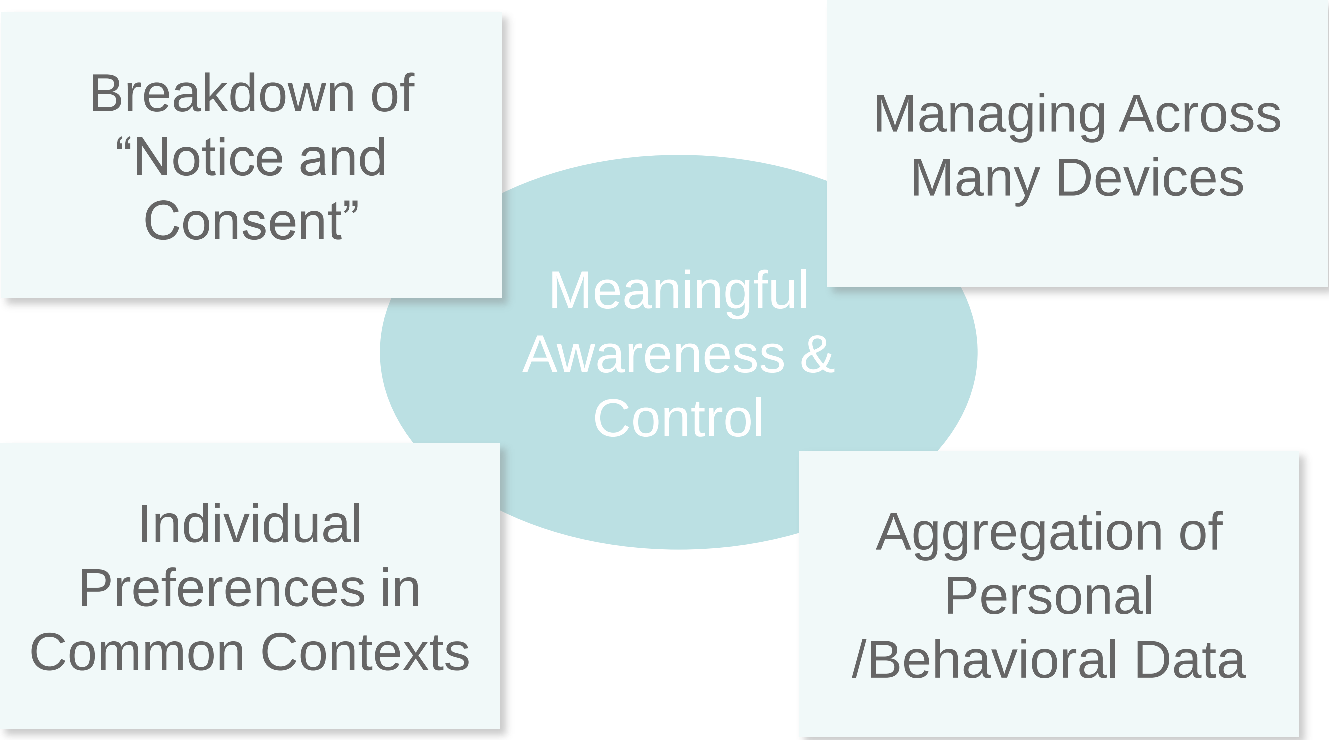
See http://www.internetsociety.org/collaborativesecurity

Privacy

Privacy and IoT: Data is a Double-Edged Sword

- The data streams /analytics that drive the value IoT can also paint very detailed and intrusive pictures of our lives.
- Expands the feasibility / reach of surveillance and tracking.
- Redefining the debate about privacy issues
  - Can dramatically change the ways personal data is collected, analyzed, used and protected.
- Implications on our:
  - Basic rights
  - Sense of personal safety and control
  - Ability to trust the Internet and devices connected to it.

Different Dimensions of Privacy Challenges in IoT



Meaningful Awareness & Control

Breakdown of “Notice and Consent”

Managing Across Many Devices

Individual Preferences in Common Contexts

Aggregation of Personal /Behavioral Data

Cross-Border Data Flows

Global Data Protection

Discrimination

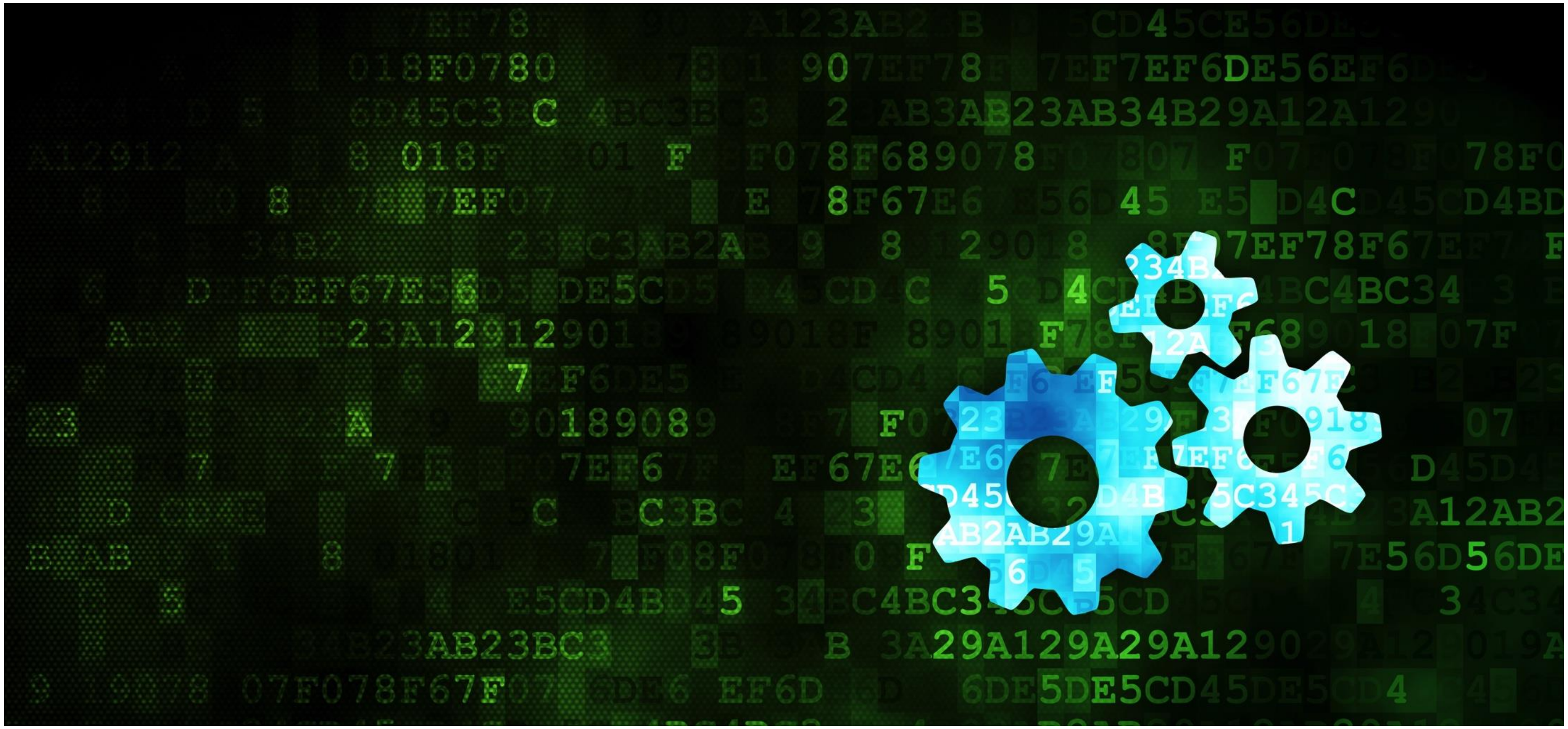
Law Enforcement

Enhancing Privacy in IoT

- *Strategies need to be developed that respect individual privacy choices across a broad spectrum of expectations, while still fostering innovation in new technology and services.*
  - Traditional on-line privacy models may not fit.
- Adapting/adopting basic privacy principles, suc
  - Transparency/Openness
  - Meaningful Choice
  - Data Minimization
  - Use Limitation

    - Among others..

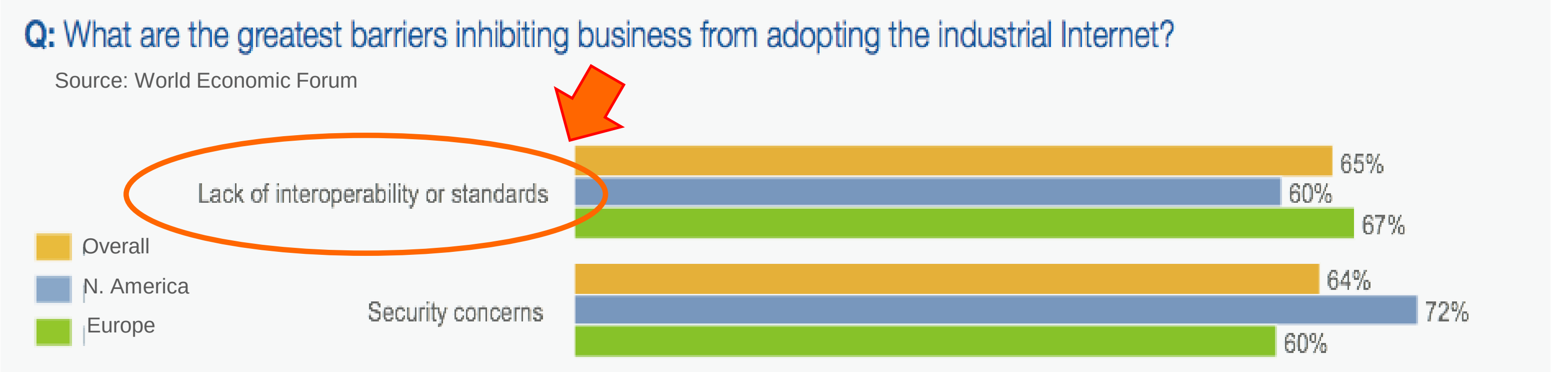
Interoperability & Standards



I&S: Not Just a Tech Challenge, It's a Market Issue

40% Interoperability is necessary to create up to 40 percent of the economic value generated by IoT
-- McKinsey Global Institute

Efficiency
Scale
Market Value



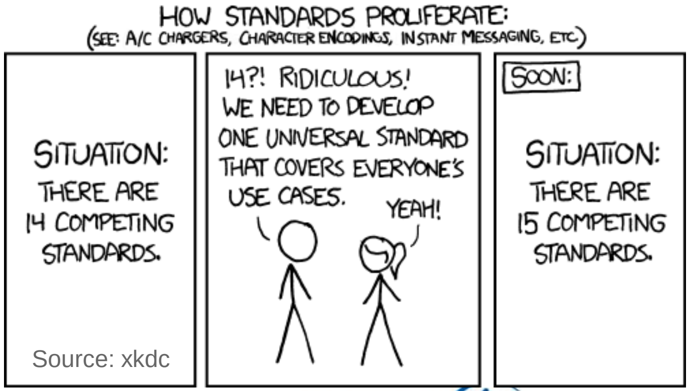
Q: What are the greatest barriers inhibiting business from adopting the industrial Internet?

Source: World Economic Forum

Interoperability / Standards Considerations

- Complex / Dynamic Service Delivery Chains and Use Cases
- Land Rush and Schedule Risk
- Proliferation of Standards Efforts
  - Industry coalitions, alliances, SDOs, proprietary development etc.
    - Can overlapping efforts be avoided without undue coordination overhead?
- Where is Interoperability Needed?
- Reusable Building Blocks
- Best Practices and Reference Models

Ultimately about advancing innovation and user choice


HOW STANDARDS PROLIFERATE:
(SEE: A/C CHARGERS, CHARACTER ENCODINGS, INSTANT MESSAGING, ETC.)
SITUATION: THERE ARE 14 COMPETING STANDARDS.
14?! RIDICULOUS! WE NEED TO DEVELOP ONE UNIVERSAL STANDARD THAT COVERS EVERYONE'S USE CASES.
YEAH!
SOON:
SITUATION: THERE ARE 15 COMPETING STANDARDS.

Source: xkdc

Legal, Regulatory, and Rights Issues

Legal, Regulatory, and Rights Issues

- Data Protection and Crossborder Data Flows
- IoT Data Discrimination
- IoT Devices as Aids to Law Enforcement and Public Safety
- IoT Device Liability
- Proliferation of IoT Devices Used in Legal Actions
- Regulatory, Legal, and Rights Issues Summary
  - Internet Society principles of promoting a user’s ability to *connect*, *speak*, *innovate*, *share*, *choose*, and *trust* are core considerations for evolving IoT laws and regulations that enable user rights.

Emerging Economy and Development Issues

Emerging Economy and Development Issues

- Infrastructure resources
- Investment
- Technical and Industry Development
- Policy and Regulatory Coordination

Closing Thoughts

- IoT is happening now, with tremendous transformational potential
- But the challenges must be addressed to realize the opportunities and benefits
  - Significant. Real. But not insurmountable
  - Solutions won’t found by simply pitting promise vs. peril
- **It will take Informed engagement, dialogue**, and **collaboration** across a range of stakeholders to find solutions and to plot the most effective ways forward.

the Internet is for everyone

Thank You
Muchas Gracias

Shernon Osepa
osepa@isoc.org

Internet Society™

InternetSociety.org