A policy framework for an open and trusted Internet

ISOC UK Webinar
14 February 2017
The Challenge

• **Diminishing trust:** data breaches, uncertain data usage, cybercrime, surveillance etc

• **Policymakers challenge:** How to embrace digital revolution while ensuring safety and security for citizens.

**ISOC:**

• Trust is cornerstone of connectivity

• Requires collective responsibility and collaboration
An ‘open and trusted Internet’ a globally interoperable Internet that cultivates innovation and creates opportunities for all.
• **User trust:** How and why users – including government, private sector and citizens - trust the Internet, and how to build that trust.

• **Technologies for trust:** Technical building blocks for trusted networks, applications and services.

• **Trusted networks:** The Internet is an ever-evolving collection of interconnected networks with distributed ownership and control. Trust is the glue that keeps networks connected and exchanging data.

• **Trustworthy ecosystem:** How the Internet is governed and how it deals with Internet issues.
User Trust

- Human Rights
- Communications confidentiality
- Privacy
- Consumer Protection
- Control over data
- Transparency in policymaking
- Legal certainty
- Enforcement and remedies
- Non discrimination
- Watchdogs and Whistle-blowers
Governments should:
- Empower users to adopt own technical measures of protection
- Encourage open development & open access to “easy-to-use” tools to communicate confidentially
- Encourage end-to-end encryption
• **Government should NOT:**
  - Limit use/access to encryption
  - Mandate “backdoors” or vulnerabilities, including third-party access to unencrypted data/encryption keys
  - Weaken/undermine encryption standards
  - Compel or pressure an entity to act against these tenets

  - Users should have option to use strongest encryption available
• (Cyber)security:
  - should advance economy and social prosperity
    – not hinder growth, innovation, development
  - Embrace expertise of all stakeholders & work collaboratively
  - Integrate human rights – safety and security with individuals’ rights
  - Defines and implements where they have most impact
  - Cross-border collaboration is essential
• **Connecting networks and sending traffic – Governments should:**
  
  – Not mandate data localization or prescribed traffic routes
  
  – Encourage regional and international companies to participate in local interconnection & peering
  
  – Foster investment in infrastructure for resiliency
  
  – Provide legal environment that supports competitive markets in online services
  
  – Support open technical standards [OpenStand principles]
• **Inclusiveness and transparency:**
  - basis of legitimacy – those affected are involved in making it
  - essential part of effective process

• **Shared responsibility:**
  - Collective stewardship of the Internet and open standards its technologies are based on.
Effective decision-making and implementation:
- Based on broad open/deliberative process
- Stakeholders who are part of the process work harder to implement it

Collaboration, distributed and interoperable governance:
- Autonomy with dialogue and mutual participation between organizations involved in internet governance.
Topics on preliminary agenda

• Editorial responsibility for online content - platform neutrality, recommender systems and the problem of 'fake news’
• Collaborative security
• User-Trust, with regard to longevity and security of IoT devices
• Search ranking technologies
• Round table on current issues related to user trust in Europe
Other topics to possibly raise during discussion

• Privacy, Data breaches, Digital Literacy

• Government surveillance powers – IP Act
• Impact of nation-first, anti-globalisation (Brexit)
• Governance of platform economy (abuse of ‘tech’ company status to avoid regulations)

• UNESCO Internet Universality Indicators – User Trust indicators