Internet Fragmentation

An Overview

Christine Arida | MEAC-SIG 2016

Beirut, Lebanon | 8-12August 2016

Original Shared Vision of an Unfragmented Internet

- Universal connectivity among the willing …

  Every device on the Internet should be able to exchange data packets with any other device that is willing to receive them.

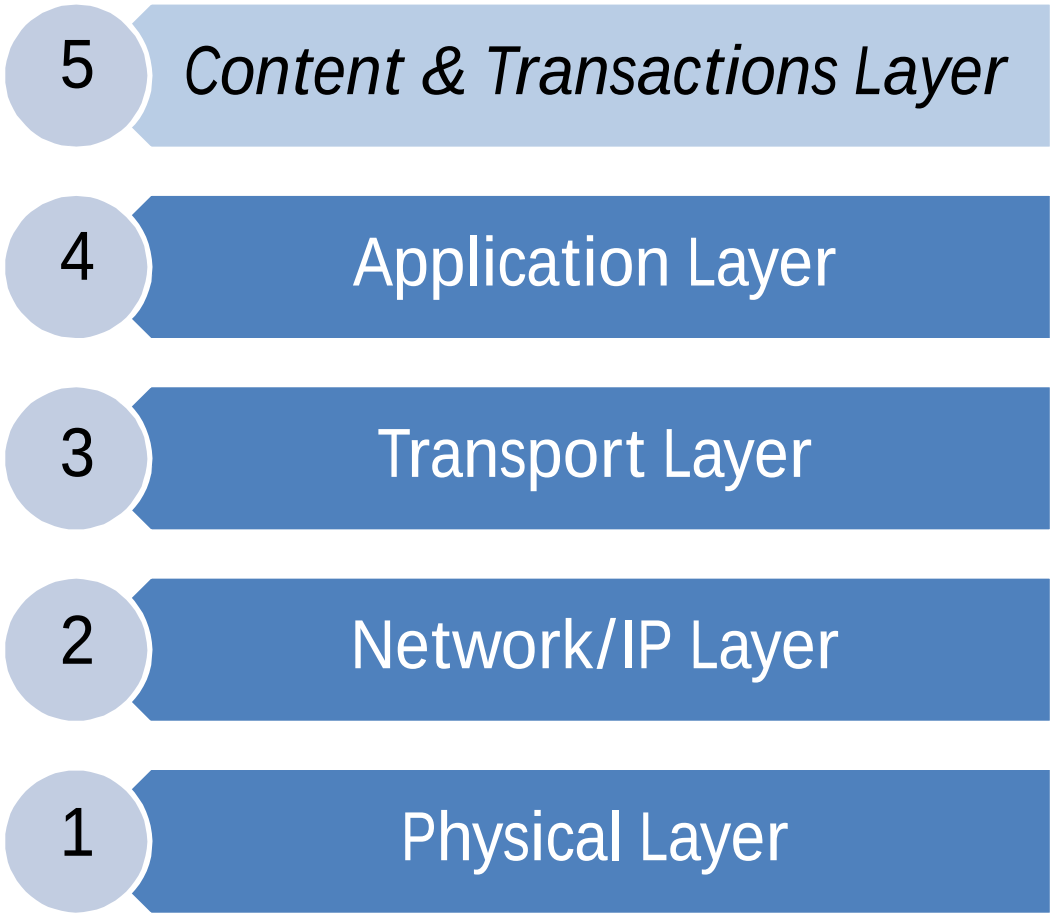
- Interoperability through the deployment of common protocols
- Seamlessly coherent on an end to end basis regardless of location

Baseline for an Open Internet

- Global reach and integrity
- General purpose
- Permission-less innovation
- Universal accessibility
- Interoperability
- Stakeholders collaboration
- Reusability of technology as building blocks
- No permanent favourites

Constraints on such Internet usage by technical malfunction, government policies or commercial practices can cause Internet fragmentation.

The Internet Layered Stack of Functionalities



Three Forms of Fragmentation

- **Technical Fragmentation**:

  Conditions in the underlying infrastructure that impede the ability of systems to fully interoperate and exchange data packets and of the Internet to function consistently at all end points. (layers 1-4)

- **Governmental Fragmentation**:

  Government policies and actions that constrain or prevent certain uses of the Internet to create, distribute, or access information resources. (layer 5 – may target lower layers)

- **Commercial Fragmentation**:

  Business practices that constrain or prevent certain uses of the Internet to create, distribute, or access information resources. (layer 5 – may target lower layers)

Variability of Fragmentation

- **Occurrence**:

  Potential or existing fragmentation
- **Intentionality**:

  Deliberate or unintended action
- **Impact**:

  Deep, structural and including large activities (possibly the Internet as a whole); or shallow, malleable and narrowly bounded
- **Character**:

  Positive, negative, or neutral

Technical Fragmentation

- Original Internet concept of universal connectivity:
  - Every device on the Internet should be able to exchange packets with any other device
  - No device compelled to engage
- Original concept eroded due to technical evolutionary trends (intentionally or a as by-product) in four main areas:
  - Addressing
  - Interconnection
  - Naming
  - Security

Technical Fragmentation Cases

1. Network Address Translation 2. IPv4 and IPv6 incompatibility and the dual-stack requirement	Addressing
3. Routing corruption 4. Firewall protection 5. Virtual private network isolation and blocking 6. TOR “onion space” and the “dark web”	Interconnection
7. Internationalized Domain Name technical errors 8. Blocking of new gTLDs 9. Private name servers and the split-horizon DNS 10. Segmented Wi-Fi services in hotels, restaurants, etc. 11. Possibility of significant alternate DNS roots	Naming
12. Certificate authorities producing false certificates	Security

Sustained Delays or Failure to Move from IPv4 to IPv6

- IPv4: 32-bit address represented as 4 decimal values separated by periods, each with a value ranging from 0 to 255, allowing for up to 4.3 billion terminations on the Internet (example 163.121.2.5)
- Not enough numbers to serve the growing Internet? … New address system - IPv6
- IPv6: 128-bit address space, allowing for 340 trillion trillion trillion endpoints
- IPv4 & IPv6 not compatible and run in parallel (dual-stack mode)
- Only 4% of the Internet servicing IPv6 usage
- IPv4 space depleted at RIRs
- Enormous anticipated demand triggered by IoT and virtual machines
- Fragmentation risk due to lagging IPv6 transition and IPv4 & IPv6 Internets not interworking
- Dual-stack implementation encouraged at ISPs and device makers

Widespread Blocking of New gTLDs

- The domain name system DNS: originally using 8 generic top level domains gTLDs and ~200 country code top level domains ccTLDs (limited number of additional gTLDs added from 2000 to 2011)
- New gTLD program launched (2012): 853 new domains delegated and 480 in process (as of December 2015)
- Approval of .xxx gTLD for pornography in 2011 – Announcement by many governments to block the domain
- Increased gTLD blocking implies more fragmentation

Significant Alternate Root Systems

- Same names map to different servers
- Users directed to a server pretending to be the legitimate destination
- Alternate root with significant government backing could be the mother of all fragmentations
- A possibility that was raised in the WSIS negotiations (geopolitical context)

Governmental Fragmentation

- Global public Internet divided into digitally bordered “national Internets”
- National segmentation by establishing barriers that:
  - Impede Internet technical functions, or
  - Block the flow of information and e-commerce over the infrastructure
- Debate to balance demands of national sovereignty with transnational cyberspace (Internet global commercial use 1990)
- Governments and IGOs discussing the need for new mechanisms to strengthen the hands of sovereign states with respect to the Internet
- Other views in favour of industry self-regulation with “light-touch” approach by governments
- Limited government intervention considered major reason why Internet has grown rapidly in the US

Governmental Fragmentation

- Proposals made for innovative forms of global multistakeholder governance
- Open, free and unfragmented Internet seen as universal value and enabler of worldwide economic growth and development
- Yet Internet users live within national borders overseen by governments
- Physical Internet servers operate under jurisdictions of countries
- Governments embed the Internet into public authority frameworks

Governmental Fragmentation Cases

1. Filtering and blocking websites, social networks or other resources offering undesired contents 2. Attacks on information resources offering undesired contents	Content and Censorship
3. Digital protectionism blocking users' access to and use of key platforms and tools for electronic commerce	E-commerce and Trade
4. Centralizing and terminating international interconnection 5. Attacks on national networks and key assets 6. International frameworks intended to legitimize restrictive practices	National Security

Governmental Fragmentation Cases

7. Local data processing and/or retention requirements 8. Architectural or routing changes to keep data flows within a territory	Privacy and Data Protection
9. Prohibitions on the transborder movement of certain categories of data	Data Localization
10. Strategies to construct “national Internet segments” or “cybersovereignty”	Fragmentation as an Overarching National Strategy

Filtering and Blocking due to Content

- Interplay between free flow of information and national sovereignty
  - Every individual has *"the right to seek, receive and impart information and ideas through any media and regardless of frontiers"* - Universal Declaration of Human Rights
  - States have the right to cut off (in accordance with national law) communications, dangerous to security or against law, public order or decency – ITU Constitution

Filtering and Blocking due to Content

- How are international human rights laws to be applied on the Internet? Progress made in international discussions
- Simultaneously national activities of content regulation and censorship have grown steadily
  - Filtering cross-border information flows (DNS, IP or keywords)
  - Laws and regulations legitimizing filtering actions; lawful interception; longstanding speech restrictions
  - Forced registration of websites, bloggers and users
  - Revoking ISP licenses
  - Denying access to social networks
- Damage restricted to particular user population and to specific content
- A human rights centered analysis needed (the right to freedom of expression and access to information)

Digital Protectionism

- Shift to an Internet economy - worth $4.2 trillion $ by 2016 in G-20 countries only
- Strong relation between Internet openness and wealth creation
- Predominance of US technology companies
- Governments tempted to preference national/regional players and digital spaces
- Trying to cope with challenges to national identity & independence, tax bases, citizens rights … etc.
- Despite tension, there are signs of progress in opening markets on the Internet (example: WTO, OECD, EU …)
- Blocking user access to platforms and tools of e-commerce constitutes and example of fragmentation

Data Localization

- Limitation on storage/flow of data and data managing companies bases on geography/nationality
  1. Data be processed by local entities
  2. Data be stored locally – “resident”
  3. Data flow restricted to a certain territory (network architectures/routing restrictions)
  4. Discriminatory policies based on company’s country of origin
  5. Restriction on transborder movement of certain types of data (prior consent needed)
- Motivated by information sovereignty, security and privacy
- Job made easier for digital surveillance
- Not successful as an economic strategy

Strategies for “National Internet Segments” or “Cybersovereignty”

- Suggesting an Internet architecture organized into segmented stand-alone national domains with interconnecting gateways
- Discrete cyberspaces of content and transactions controlled by national policies
- Several proposals for intergovernmental bodies to govern the Internet
- Different approaches to ‘Enhanced Cooperation’ – including at the national level
- A failure of the transition process of the IANA stewardship function could encourage more governmental fragmentation actions
- Open and unfragmented Internet continue to be promoted – NETmundial Multistakeholder Statement 2014
- The need for watchfulness, dialogue and cooperation to avoid a future where the Internet stops to be a global village

Commercial Fragmentation

- Commercial practices by technology companies that contribute to Internet fragmentation
- The organization of specific markets and digital spaces and the experiences of users that choose to participate in them, possible impacting the technical infrastructure and operational environments for everyone
- Five issue-areas categorized:
  - Peering and standardization
  - Network neutrality
  - Walled gardens
  - Geo-localization and geo-blocking
  - Infrastructure-related intellectual property protection.

Commercial Fragmentation Cases

1. Potential changes in interconnection agreements 2. Potential proprietary technical standards impeding interoperability in the IoT	Peering and Standardization
3. Blocking, throttling, or other discriminatory departures from network neutrality	Network Neutrality
4. Walled Gardens	Walled Gardens
5. Geo-blocking of content	Geo-localization and geo-blocking
6. Potential use of naming and numbering to block content for the purpose of intellectual property protection	Infrastructure-related intellectual property protection.

Walled Gardens

- Concept expanded with the spread use of smart devices and the “App Economy” – think of the services/transactions we now prefer to use/conduct on dedicated Apps rather than browsers
- At the level of search engines, they cannot index information on social and commercial platforms like Twitter, Facebook, etc.
- Providers offer high quality customer experience, at the expense of providing exclusive content, customer lock-in (loyalty) and provider having complete control over its digital space
- Growing share of digital life retreat behind companies’ walled gardens constitutes a form of fragmentation on the Internet

Geo-blocking

- Geo-localization is identifying user location by mapping his device IP address → Decide which kind of content will be served to the user based on his geographical location: geo-targeting and geo-blocking
- Geo-blocking: content inaccessible in certain geographic locations mainly to protect Intellectual Property or local media licenses, or due to legal compliance (e.g. online gambling)
- Frustrating to user, experiencing restrictions on full access to publicly available online content
- Denial of access to content available on the Internet based on a location is considered a form of fragmentation

Conclusion

- Out of 28 examples of fragmentation cases, 10 issues merit further attention – “top 10”:
- Fairly pressing or worth keeping a close watch of
- Worth examining in greater detail
- Potential for progress through multistakeholder dialogue and collaboration

1. Sustained delays or failure to move from IPv4 to IPv6
2. Widespread blocking of new gTLDs
3. Significant alternate root systems
4. Filtering and blocking due to content
5. Digital protectionism
6. Local data processing and/or retention requirements
7. Prohibitions on the transborder movement of certain categories of data
8. Strategies for “national Internet segments” or “cybersovereignty”
9. Walled gardens
10. Geo-blocking

Conclusion

Six sets of challenges stand out as pressing and worth analyzing through multi-stakeholder dialogue and cooperation:

- Fragmentation as Strategy
- Data Localization
- Digital Protectionism
- Access via Mutual Legal Assistance Treaties (MLATs)
- Walled Gardens
- Information Sharing

Way Forward …

- Develop holistic understanding and top-level mapping of landscape that take note of *variations*
- Identify “bad” fragmentation cases that merit “deep dive” analysis
- Develop methodology for assessing risks, costs/benefits
- Undertake global multistakeholder dialogue to raise awareness and set conditions that could evolve toward shared solutions
- Proceed with collective awareness of conditions arising across the infrastructure and its usage

This presentation is based on:

The World Economic Forum's Future of the Internet Initiative White Paper

"Internet Fragmentation: An Overview"

by William J. Drake, Vint Cerf, Wolfgang Kleinwächter

January 2016

http://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf

ANY QUESTIONS???