The Expanding Landscape of Internet Governance:

Why Network Operators Need a Global View

John Curran

NANOG 89 – October 2023 – San Diego CA USA

A bit about me

John Curran

- President and CEO of *American Registry for Internet Numbers* (ARIN).

  (Provided for identification purposes only – ARIN's Board of Trustees has not reviewed this presentation: it contains my thoughts & advice to network operators, whereas ARIN's mission is the opposite; i.e., to follow the guidance of the networking community in providing Internet number registry services for the region.)

- Previously CTO at Bolt, Beranek, and Newman (BBN), working on many early Internet projects CSNET, NSF Network Service Center (NNSC), NEARNET, etc.
- IETF Participant – as author/contributor to various Internet Drafts / RFCs, was Area Director for the Ops/Network Management Area, served on IPng (IPv6) Directorate, etc.
- Ran two US nationwide ISPs (BBN/GTE Internetworking and XO Communications).
- Ran a highly-secure hosting/datacenter for sensitive clients and governments.
- Been active in *Internet Coordination* & *Internet Governance* activities for more than 30 years.

Internet Coordination versus Governance

Internet Coordination refers to the technical and operational management of key Internet resources, such as domain names, IP addresses, and protocol parameters. It involves the implementation of standards, allocation of resources, and maintenance of essential functions that enable the Internet to operate smoothly.

The coordination occurs via open and transparent processes in which all parties may participate – often known as the "*Multistakeholder Model*".

Organizations that have evolved from the earliest days of the Internet – e.g., the Regional Internet Registries (RIRs), Internet Corporation for Assigned Names and Numbers (ICANN), Internet Assigned Numbers Authority (IANA), W3C (World Wide Web Consortium, Internet Engineering Task Force (IETF), and NANOG – help structure and drive this technical coordination.

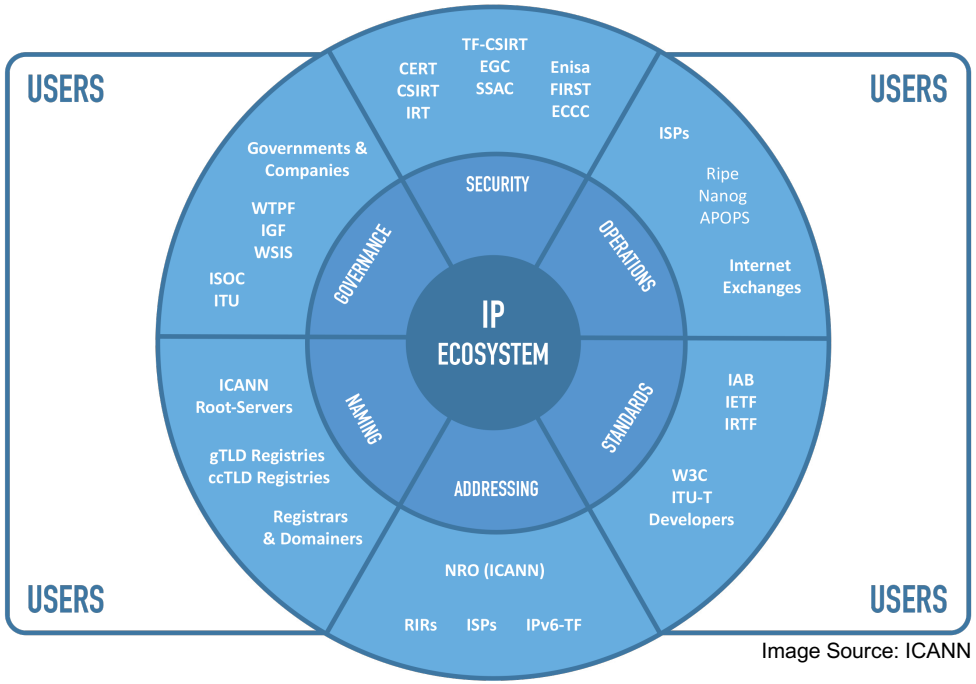


Image Source: ICANN

Internet Governance *is a broader concept that encompasses the overarching norms, policies, and regulations that guide the usage of the Internet.*

What this talk is about…

The ongoing evolution of the Internet from today's massive commercial activity into something more integral to society –

… including some of the more likely consequences that network operators will face as the various ***Internet Governance*** *bear fruit.*

What this talk is not about:

- Virtual Reality (VR), Augmented Reality (AR), or the Metaverse
- Misinformation & Content Moderation
- Encryption, Quantum computers, and Post-Quantum Cryptography (PQC)
- Internet of Things (IoTs)
- Artificial Intelligence (AI) & Natural Language Processing (NLP) & Large Language Models (LLMs)
- *Application of any particular law or regulation to your organization*

Internet Governance & Governments

*"A working definition of **Internet governance** is the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet."*

(Paragraph 34, World Summit on the Information Society (WSIS) Tunis Agenda, 18 November 2005)

Note: a traditional take on the "respective role of government" in society includes duties such as –

- Establishing common norms of conduct or behavior for society
- Having the use or threat of force to compel adherence to laws and regulation
- Engaging in the management of public resources for the common good

Internet Governance & Governments

Duties often cited stemming from "the respective role of governments" with respect to the Internet –

- National Defense: Protecting critical online infrastructure from cyber threats and espionage, and cyber incident response coordination.
- Providing Public Services: Ensuring that the Internet is accessible & affordable to all citizens and supporting initiatives that reduce the digital divide.
- Regulating the Economy: Overseeing e-commerce, digital taxation, and competition among online businesses.
- *Maintaining a Healthy Society: Regulating online conduct to reduce spread of misinformation and protect minors from inappropriate content.*
- *Protecting Individual Rights: Safeguarding privacy and freedom of expression online and protecting against discrimination and harassment.*
- *Ensuring Safety and Order: Implementing cybersecurity measures for Internet infrastructure, combating cybercrime, and mandating cooperation for law enforcement.*

Some government's expectations regarding their perceived public policy obligations can be particularly challenging to address given the globally interconnected nature of the Internet.

Why Internet Governance?

Potential for Economic Impact

In *2016*, Deloitte undertook a comprehensive analysis of the potential impact to an economy's gross domestic product (GDP) as a result of a significant Internet disruption. Some key findings from the report[1]:

- *Widespread Impact: Disruptions to Internet-based services and infrastructure have widespread impacts on people and the economy. Even partial disturbances affect productivity, sour business confidence, and lead to lost opportunities.*
- *Economic Loss by Connectivity Level: For a highly Internet-connected country, the per-day impact of a temporary shutdown would be on average $23.6 million per 10 million population. For medium and low Internet connectivity economies, the average estimated GDP impacts amount to $6.6 million and $0.6 million per 10 million population, respectively.*

[1] "The Economic Impact of Disruptions to Internet Connectivity", Deloitte LLP, 2016, https://www.deloitte.com/global/en/Industries/tmt/perspectives/the-economic-impact-of-disruptions-to-internet-connectivity-report-for-facebook.html

Why Internet Governance?

Potential Impact to National Security

- *Hackers infected 70 percent of storage devices that record data from D.C. police surveillance cameras eight days before President Trump's inauguration, forcing major citywide reinstallation efforts. City officials said ransomware left police cameras unable to record between Jan. 12 and Jan. 15. The cyberattack affected 123 of 187 network video recorders in a closed-circuit TV system for public spaces across the city.* [2]
- *Hackers have been penetrating the computer networks of companies that operate nuclear power stations and other energy facilities, as well as manufacturing plants in the United States and other countries. This includes Wolf Creek Nuclear Operating Corporation, which runs a nuclear power plant near Burlington, KS, according to an urgent joint report from DHS & FBI.*[3]

[2] "DC police surveillance cameras were infected with ransomware before inauguration", Ars Technica, 27 January 2017, https://www.washingtonpost.com/local/public-safety/hackers-hit-dc-police-closed-circuit-camera-network-city-officials-disclose/2017/01/27/d285a4a4-e4f5-11e6-ba11-63c4b4fb5a63_story.html

[3] "Hackers Are Targeting Nuclear Facilities, Homeland Security Dept. and F.B.I. Say", New York Times, 6 July 2017, https://www.nytimes.com/2017/07/06/technology/nuclear-plant-hack-report.html

Why Internet Governance?

Impact to Public Services

- *A ransomware attack on a California-based health care system forced some of its locations to close and left others to rely on paper records. Prospect Medical Holdings, operating 16 hospitals and more than 165 clinics and outpatient centers in Connecticut, Pennsylvania, Rhode Island and Southern California, announced the cyberattack.* [4]
- *In late April 2022, after weeks of major ransomware attacks, Costa Rica declared a state of emergency. The Costa Rica government refused to pay the ransom and scrambled to get systems and services back online. The Costa Rican Treasury told civil servants that the attack had halted automatic payment services. Workers were warned the government was unable to pay them on time. Instead, they would need to apply for their salaries by email, or by hand on paper. The attack also affected the country's foreign trade. It disrupted its tax and customs systems, which led to import and export logistics collapse.* [5]

[4] "Ransomware Attack Disrupts Health Care Services in at Least Three States", New York Times, 5 August 2023, https://www.nytimes.com/2023/08/05/us/cyberattack-hospitals-california.html

[5] "Costa Rica state of emergency declared after ransomware attacks", Security Intelligence, November 2022, https://securityintelligence.com/news/costa-rica-state-emergency-ransomware/#

Why Internet Governance?

Human Impact

- *Equifax, one of the three largest consumer credit reporting agencies in the United States, announced in September 2017 that its systems had been breached and the sensitive personal data of 148 million Americans had been compromised. The data breached included names, home addresses, phone numbers, dates of birth, social security numbers, and driver's license numbers. The credit card numbers of approximately 209,000 consumers were also breached.* [6]
- *More than 200 victims of sex trafficking were rescued during a nationwide enforcement campaign including the identification or arrest of more than five dozen suspected human traffickers and 126 individuals accused of child sexual exploitation and trafficking offenses. The FBI-led "Operation Cross Country," also located 59 minor victims of child sex trafficking and sexual exploitation, and another 59 children who had been reported missing.* [7]

[6] "Equifax Data Breach", Electronic Privacy Information Center, https://archive.epic.org/privacy/data-breach/equifax/

[7] "Operation Cross Country XIII Leads to Identification/Location of Adolescent Victims", US FBI, 1 August 2023, https://www.fbi.gov/news/press-releases/operation-cross-country-2023

Why Internet Governance?

Human Impact (cont.)

- *"The ransomware attack unfolding on 2 July 2021 against Kaseya Ltd, a Miami-based software producer, was the world's largest to date. As an indiscriminate supply chain attack, this case brings into sharper focus the extent of the harm inflicted by ransomware to society as a whole. The attack was disruptive for everyone using Kaseya services directly or indirectly, including nurseries, schools, pharmacies and supermarkets in 17 countries. … The attack against Kaseya combined a trusted means of deploying automatic software — via a managed service provider — with a near-impossible-to-defend-against attack vector. … In a matter of minutes, it caused harm on an unprecedented scale, hitting around 1,500 companies and thousands of victims around the world, from businesses and municipalities in the United States to Australian organizations. In Sweden, a large food retailer was forced to close 800 shops over the weekend, while the State Railway and a pharmaceutical chain also suffered disruptions. Eleven schools and more than 100 nurseries fell victim to this attack in New Zealand."* [8]

[8] "What we learned from the Kaseya attack: recommendations for a human-centric approach to curb ransomware", CyberPeace Institute, August 2021. https://cyberpeaceinstitute.org/publications/what-we-learned-from-the-kaseya-attack-recommendations-for-a-human-centric-approach-to-curb-ransomware/

Why Internet Governance?

Human Impact (cont.)

- *"Hackers have stolen roughly $1.9 million from South Korean cryptocurrency platform KLAYswap after they pulled off a rare and clever BGP hijack against the server infrastructure of one of the platform's providers. The BGP hijack hit KakaoTalk, an instant messaging platform popular in South Korea. South Korean cybersecurity firm S2W said that the attackers used a BGP hijack as a way to serve a malicious version of KakaoTalk's JavaScript SDK file … modified to include additional code at the end of the file that, once loaded inside a user's browser, would wait for them to initiate a transaction on the KLAYswap website, such as an asset deposit, swap, or withdrawal. KLAYswap said that during a period of two hours—from 11:30 to 1:30, on February 3—the attacker stole the equivalent of 2.2 billion of Korean won (~$1.9 million) worth of various cryptocurrency assets."* [8]

[9] "KlaySwap crypto users lose funds after BGP hijack", The Record, February 2022, https://therecord.media/klayswap-crypto-users-lose-funds-after-bgp-hijack

Governments and Internet Coordination

"How do we fulfill our public policy obligations for a safer Internet, including measures such as filtering network traffic & DNS for content or security reasons, requiring user ID verification for website access, supporting law enforcement's requirement for access to stored data and/or packet inspection for cybersecurity and national defense reasons, etc.?"

"It appears that the Internet technical community protocol standards and registry policies are effectively mandatory – as government participants, shouldn't we be able to fulfill our public policy objectives via changes to the technical policies and standards?

The Internet technical community invests significant resources explaining the "voluntary" nature of Internet standards and practices, but the reality is that they don't appear to be voluntary – at least not when viewed by the perspective of governments. For example:

- *In order to interconnect successfully, one has to use the IETF's protocols (IP, DNS, routing, web)*
- *To make use of the associated registries, one has to follow ICANN and RIR policies (for DNS and Internet number resources respectively)*

Governance Trajectory for the Internet

1. Governments seek to control the affairs of those within their territory as a furtherance of their public policy objectives, and this includes all manner of endeavors *including the Internet*.
2. When it comes to the Internet, government inability to fulfill their perceived public policy goals – due to lack of a clear framework for cooperation with the Internet technical community – has not caused them to desist.
3. Lacking a clear route via Internet Coordination to achieve their perceived public policy objectives for the Internet, governments will instead pursue such via more traditional national and intergovernmental (bilateral, regional and global) initiatives.
4. Such governmental efforts will not necessarily make use of multistakeholder processes, nor norms/standards from those organizations doing Internet coordination today.
5. The ability of service providers of all types (ISP, hosting, DNS, cloud, content, social media, etc.) to continue to successfully operate a richly connected Internet – once made subject to numerous disjointed regulatory measures and associated norms – is unknown and may be challenging if the current ad hoc Internet governance approach is followed to its logical conclusion.

Examples of Internet Governance to date

Maintaining a Healthy Society: ***Protection of Minors*** –

- US Children's Online Privacy Protection Act (COPPA), *COPPA 2.0, KOSA*
- UK Digital Economy Act 2017
- US States – Louisiana, Arkansas, Texas, California, Utah, …

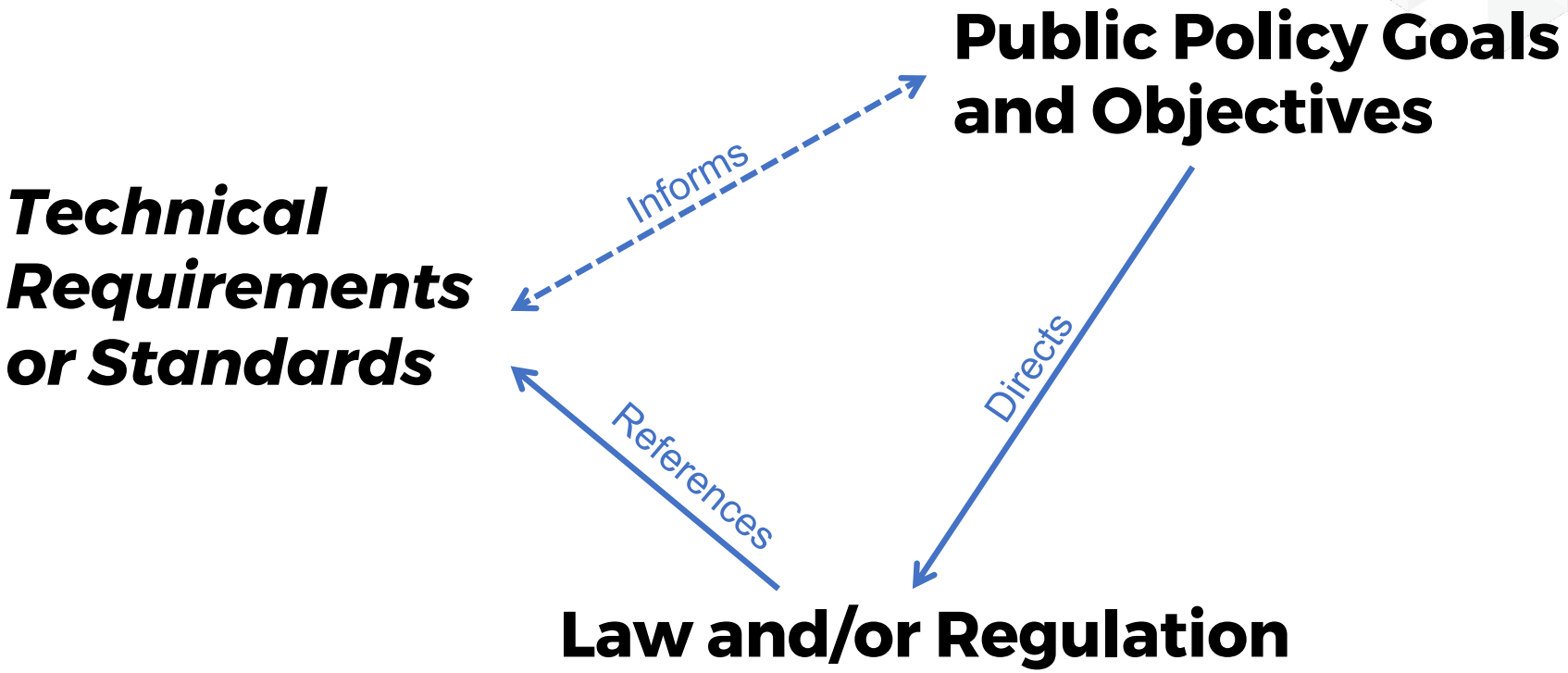
Protecting Individual Rights: ***Personal Data Privacy*** –

- EU's General Data Protection Regulation (GDPR)
- Canada's Personal Information Protection and Electronic Documents Act (PIPEDA)
- EU-US Data Privacy Framework (DPF)
- US States: California Consumer Privacy Act (CCPA), Virginia Consumer Data Protection Act (CDPA), Colorado Privacy Act (CPA), …

Ensuring Safety & Order: ***Cybersecurity & Electronic Evidence*** –

- US CLOUD Act & DAAs (UK's Investigatory Powers Act, Australia's Assistance and Access Act)
- EU E-Evidence Act
- *CA Bill C-26, An Act Respecting Cyber Security (ARCS)*
- *United Nations "Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes"*

Interaction of Policy and Standards



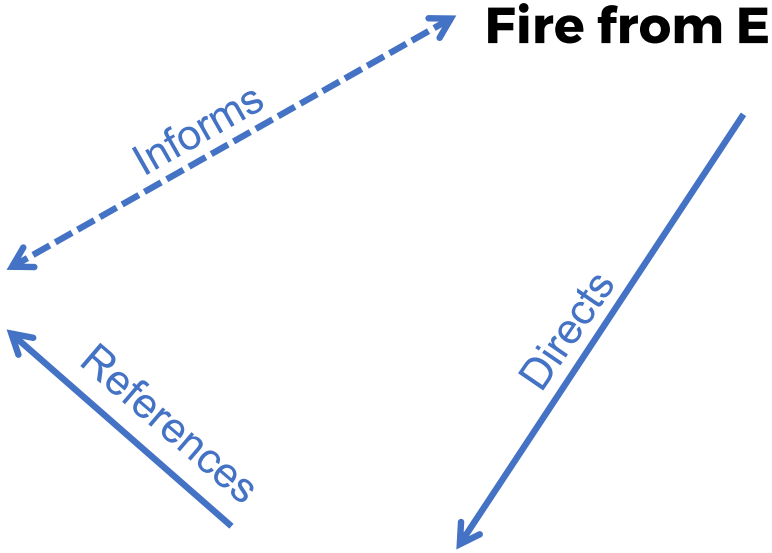
Governance in other domains

It is worth noting that industry and governments working together in their respective roles to advance safety and security of systems is not particularly new or difficult…

Industry	Trade Association	Technical Standards Referenced by Law or Regulation
Automotive	Society of Automotive Engineers (SAE)	Vehicle safety, emissions, fuel efficiency
Highway & Transportation	American Association of State Highway and Transportation Officials (AASHTO)	Highway design, construction, maintenance, safety
Air Transport	International Air Transport Association (IATA)	Air transport safety, security, efficiency
Rail Transport	Railway Association of Canada (RAC)	Rail transport safety, efficiency
Trucking & Engines	Truck and Engine Manufacturers Association (EMA)	Emissions, safety, fuel efficiency
Aerospace	Aerospace Industries Association (AIA)	Aircraft safety, quality, environmental compliance

Referencing Technical Expertise

Goal: Buildings Not Catching Fire from Electrical Wiring



Fire & Electrical Codes

(as developed by relevant standards bodies)

Building Code – As adopted by Applicable Authority

Internet Governance

Governments are already exercising their respective roles with respect to the Internet – and most often via unilateral national regulatory actions.

When such activity is based on the use of Internet best practices and/or technical standards (e.g., IETF RFCs / BCPs), there is lower risk of adverse impact – but those that do not consider the globally interconnected nature of the Internet have the potential to be quite detrimental.

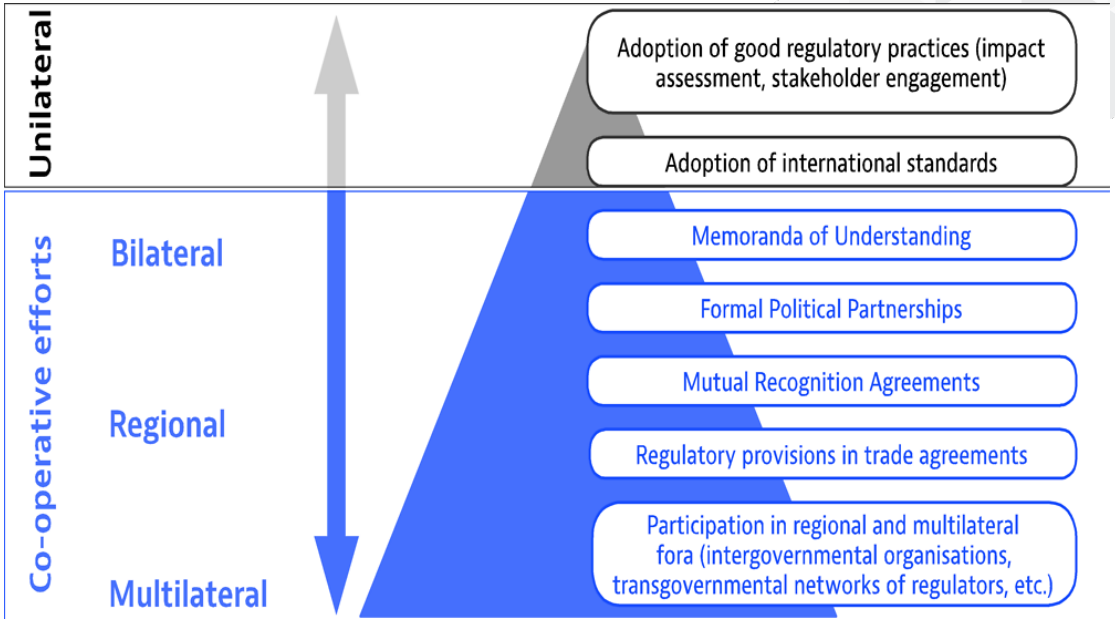


Image Source: Based on (OECD, 2013[3]), *International Regulatory Co-operation: Addressing Global Challenges*, OECD Publishing, Paris, http://dx.doi.org/10.1787/9789264200463-en.

Internet Governance – Roles

It would be helpful if there were a commonly understood set of roles for governments and the Internet technical community within the Internet Governance model –

- Recognition that the Internet is global and interconnected in nature, and therefore that the ***technical and operational global standards and practices*** that underlie it must also be global in scope – and developed via the open and transparent multistakeholder process in order to have global credibility and applicability.
- Recognition that governments have a valid role in establishing ***Internet public policy goals and objectives*** – ideally on a global basis when possible – but national (or regional) basis when otherwise necessary. This role specifically does not include the development of technical or operational standards or practices applicable to the Internet, as such activities have proven to be more suited to the Internet technical community.
- ***Recognition that respective role of governments often results in the implementation of public policy objectives through the development of appropriate national (or regional) law and regulation, and that – with respect to the Internet – such regulation should reference the global technical standards and practices developed by the Internet technical community as appropriate.***

Evolution of the Internet

Research & Educational Internet with Multistakeholder Standards *and Government Funding/Oversight*

~1995

- Government-funded Backbone -> Multiple Commercial Backbones (1995)
- Identifier administration from InterNIC -> RIRs & ICANN (1997/1999)
- Regional Techs -> NANOG (1994 -> 2010)
- IANA Stewardship Transition (2017)

Commercial Internet with Industry-led, Multistakeholder Norms, Standards, and Oversight

~2017

- Active Internet Regulation – GDPR, EU e-Evidence, US CLOUD Act, *UN Ad hoc Committee re International Cybercrime Convention*
- Growing safety and privacy concerns
- Significant industry sectors (consumer, finance, healthcare, transportation, emergency services, energy) increasingly dependent on the Internet

Public Internet with Industry-led, Multistakeholder Norms & Standards, and Governmental Oversight

Public

How shall we govern the Public Internet?

- *With recognition of the role and responsibility of governments in establishing Internet public policy goals and objectives – done on a global and multilateral basis when possible so as to avoid fragmentation – and including the development of appropriate national (or regional) law and regulation as necessary for implementation.*
- *With such efforts referencing (where appropriate) the global technical standards, norms, and practices developed by the Internet technical community via its open and transparent multistakeholder processes.*

And who knows – we might actually end up with a better Internet as a result!

Of course, success can only be achieved through active and abundant cooperation among all parties: governments, industry and trade organizations, civil society, the Internet technical community, etc.

That's where *you* come in…

Of course, you don't have to do anything…

But if you decide to do nothing, then please do me a favor and refrain from spouting remarks in the future along the lines of the following –

- *"But I didn't know this was going on!"*
- *"But I didn't know you meant me!"*
- *"But I didn't have any way to persuade my organization it was important!"*
- *"But I didn't realize I had to actually proactively engage – I thought that everyone else would just come to me!"*
- *"But I thought we had more time!"*

We have all known for years that governments would eventually become active in Internet Governance space – and it was really just a question of when…

Well, we finally know that answer – ***It's now!***

If you are with a sizable organization

It's likely that your organization is already quite aware of the increased government interest in the Internet, and may even already have a plan for engagement –

- Find out who (or what team) is running your organization's engagement program on Internet public policy matters – introduce yourself, your role, and ask to be kept informed of developments.
- Bring relevant technical content into the discussion as appropriate and encourage your organization to support use of the multistakeholder model by intergovernmental organizations dealing with Internet policy matters.
- Help formulate your organization's positions – recognizing that your organization shares fate with others on the Internet, and that the spirit of technical coordination for common benefit of all participants does not always come naturally to participants in legal/regulatory settings.

If you are with a small organization

The same goal applies here: helping guide the technical evolution of the Internet in a cooperative manner with others (such as governments) to avoid fragmentation –

- Consider participating in various Internet trade organizations to keep aware of developments and find others of similar views for coordinated action.
- Recognize the validity of governments having public policy objectives for the Internet and provide technical input to aid in their informed development to the extent feasible.
- Formulate your organization's positions, and then engage with others of similar inclination to advocate for solutions that could improve the Internet (or at least not make it worse!)

If you are an individual contributor

It is likely that the Internet will evolve into a true public infrastructure over the next few decades, but it will take significant technical innovation and coordination if we're to avoid fragmentation in the process –

- We do know of norms and best practices that can improve the Internet if widely deployed – e.g., the IETF Best Current Practice (BCP) series, the Mutually Agreed Norms for Routing Security (MANRS) initiative, etc.
- Deploy these best practices in your own network and advocate for others to do the same.
- Work in Internet technical coordination bodies on solutions to these and other challenges facing the Internet.
- Participate as an individual technical contributor when governmental consultation processes (and your available time) allow for such!

Thank you for listening!

(… and for your help going forward in keeping the public Internet stable and richly interconnected!)