Internet Governance

Who Decides What's Online?

The Meta-Question

Throughout this course, we've examined:

- **Technical controls**: DNS, BGP, throttling, DDoS
- **Platform controls**: Moderation, personalization, disinformation
- **Legal controls**: Copyright, net neutrality, demonetization

Today's question: Who has the authority to make these decisions?

A Tale of Two Internets

The Dream (1990s)

- "Information wants to be free"
- Self-governing
- Borderless
- Resistant to control

The Reality (2020s)

- Fragmented
- National borders reasserting
- Multiple competing authorities
- "The Splinternet"

What is Internet Governance?

> "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."
>
> — World Summit on the Information Society (2005)

The Key Players: Technical & Governmental

Technical Organizations

- ICANN (domain names, IP addresses)
- IETF (internet standards, protocols)
- Regional Internet Registries (RIRs)

Intergovernmental Bodies

- ITU (UN telecommunications agency)
- UN General Assembly
- Regional bodies (EU, African Union, etc.)

The Key Players: Private Sector

Platforms & Infrastructure

- Tech platforms (Meta, Google, X)
- Infrastructure providers (ISPs, CDNs)
- Standard-setting organizations

Civil Society

- Digital rights organizations
- User advocacy groups
- Academic researchers

ICANN: The Name Game

Internet Corporation for Assigned Names and Numbers

- Controls domain name system (DNS)
- Allocates IP addresses
- Manages root servers
- Founded 1998, US government oversight until 2016

Key Power: Control of the root zone file

- Can add/remove top-level domains (.com, .org, .country codes)
- Disputes over country codes become geopolitical

ICANN Case Study: .io Domain

- .io is British Indian Ocean Territory
- Popular with tech startups ("input/output")
- UK returned territory to Mauritius (2024)
- **Question**: What happens to millions of .io domains?

Governance decision with massive economic implications.

The Multi-Stakeholder Model

Core Principle: No single entity controls the internet

Four pillars:

1. **Governments**: Set policy, regulation
2. **Private sector**: Operations, innovation
3. **Civil society**: User interests, rights
4. **Technical community**: Standards, protocols

Reality: Unequal power distribution

The Multilateral Challenge

Some countries (especially Russia, China) prefer multilateral model:

- Greater government control
- ITU as primary authority
- UN-style voting among nations
- "Cyber sovereignty"

Key tension: Control vs. openness

Russia's Sovereign Internet

RuNet (2019 law):

- Required ISPs to install DPI equipment
- Government can isolate Russia from global internet
- Centralized traffic routing
- "Protecting critical infrastructure"

2024 Reality:

- Regular tests of disconnection
- Increased blocking capabilities
- VPN crackdowns
- Moving toward parallel infrastructure

China's Approach: The Great Firewall

Not just blocking—alternative governance:

- Own DNS roots
- Great Firewall (technical control)
- Cybersecurity Law (legal control)
- Data localization requirements
- "Internet sovereignty" doctrine

Exporting the model: Digital Silk Road

The EU's Third Way

Neither hands-off nor authoritarian:

- GDPR (2018): Privacy rights
- Digital Services Act (2022): Platform accountability
- Digital Markets Act (2022): Competition
- AI Act (2024): Algorithmic governance

"Brussels Effect": Rules become global standards

Case Study: The Right to be Forgotten

Google Spain v. AEPD (2014):

- EU court ruled individuals can request link removal
- Google must comply in EU
- But should removals apply globally?

2019 ruling: No global application

But: Creates compliance complexity, jurisdictional tensions

The Splinternet Hypothesis

Is the internet fragmenting?

Evidence for:

- National firewalls (China, Russia, Iran)
- Data localization laws (60+ countries)
- Regional content rules (EU DSA, Indian IT Rules)
- Divergent platform policies by region

Evidence against:

- Technical protocols still unified
- Cross-border data flows continue
- Global platforms adapt but don't split

India's IT Rules 2021

Intermediary Guidelines:

- Content takedown within 36 hours
- Traceability requirements (threatens encryption)
- Grievance officer in India
- "Significant social media intermediaries" (5M+ users)

Impact: Global platforms hiring armies of local moderators

Australia vs. Meta (2024)

Context: Stabbing video in Sydney

- Australia ordered global takedown
- Meta complied in Australia only
- Court case over extraterritorial reach

Question: Can one country's laws apply globally?

Tension: National sovereignty vs. global platform architecture

The DNS Wars

Who controls the root?

- US government historically oversaw ICANN
- 2016: Transition to "global multi-stakeholder community"
- Russia, China still skeptical

Alternative roots:

- China testing separate DNS infrastructure
- Potential for incompatible internets
- Like telephone networks before interconnection

Content Moderation Governance

Who decides what's acceptable online?

Current reality:

- Platforms set their own rules
- Governments set legal boundaries
- Users have limited input
- AI systems enforce opaquely

Emerging models:

- Oversight boards (Meta)
- Federated systems (Mastodon)
- User choice (BlueSky algorithms)

The Twitter/X Case Study

2023-2024: Platform governance in flux

- Owner changes moderation policies unilaterally
- Governments threaten/impose bans
- Users migrate to alternatives
- Advertiser pressure

Lesson: Centralized platforms = centralized governance

Cross-Border Enforcement Challenges

Problem: Internet is global, laws are national

Examples:

- French court orders vs. US First Amendment
- EU fines for global operations
- Chinese data localization vs. cloud computing
- Jurisdiction shopping by bad actors

No easy answers

The Encryption Governance Dilemma

Who decides acceptable encryption?

- US: Crypto Wars (1990s), going for encryption (2000s-present)
- UK: Investigatory Powers Act
- EU: Chat Control proposals
- Australia: Assistance and Access Act (2018)

Technical vs. Political authority

- Cryptographers: Backdoors break security
- Governments: Need access to fight crime
- Platforms: Caught in middle

Emerging Challenges for Governance

AI and LLMs:

- Who governs AI-generated content?
- Training data governance
- Algorithmic accountability
- Deepfakes and misinformation

Web3 and Decentralization:

- Blockchain governance models
- Decentralized autonomous organizations (DAOs)
- Who moderates immutable content?

The Impossibility of Universal Governance

Why it's hard:

- Different values across cultures
- Competing interests (privacy vs. security)
- Technical architecture (decentralization vs. control)
- Economic incentives (ads vs. privacy)
- Speed of change vs. slow lawmaking

Reality: Multiple governance regimes coexist

Models for the Future

Option 1: Status Quo Plus

- Multi-stakeholder model continues
- Incremental improvements
- Regional variation accepted

Option 2: Re-centralization

- Greater government role
- ITU or UN authority
- Multilateral agreements

Option 3: Radical Decentralization

- Technical solutions to governance

What We've Learned This Quarter

Technical controls → Protocol governance matters

Platform controls → Private governance is real governance

Legal controls → National laws shape global networks

Measurement → Transparency enables accountability

Circumvention → Control is never absolute

Governance → Power is contested, always

The Core Tension

Freedom vs. Safety

Privacy vs. Accountability

Innovation vs. Stability

Global vs. Local

Public vs. Private

These aren't problems to solve—they're tensions to manage.

Discussion Questions

1. Should internet governance be primarily technical or political?
2. Is the "splinternet" inevitable? Desirable?
3. Can platforms be held accountable without government control?
4. What role should users have in governance decisions?
5. How do we govern technologies (like AI) that don't exist yet?

Looking Forward

You've learned:

- How censorship works (technically)
- Why it happens (motivations)
- Who does it (actors)
- How to measure it (methods)
- How to resist it (circumvention)

Now think about: Who *should* decide?

Final Thoughts

The internet is not ungoverned—it never was.

The question is not **whether** to govern, but:

- **Who** governs?
- **How** do they govern?
- **For whom** do they govern?
- **With what legitimacy**?

These are the questions that will shape the next 30 years of the internet.

Thank You

Questions?

Office hours: [Your details]
Final projects due: [Date]

Stay curious. Stay critical. Stay engaged.