Ten Things the FCC Should Know about the Internet

kc claffy

FCC
29 may 2009

recipe for disaster

(aka “you are here”)

- We now critically depend on the Internet for our professional, personal, and political lives.
- But what do we know about it? e.g, what keeps the system stable or drives it to instability?
- Researchers and policymakers currently analyze a trillion dollar industry in the dark.
- Few data points available suggest a dire picture.
- Agencies charged with infrastructure protection have little situational awareness regarding global dynamics and operational threats.

How did we get here?

- Telephone system: 140+ years of history, including regulated data collection requirements (and profits). and a precisely defined system.

- Data networks: 40 years old, ad hoc/hack, tossed to private sector before mature, with no govt support for research or metrics (or profit), ill-defined system.

- Current academic projects either lack sustainability (iplane) or ability to dedicate resources (PlanetLab)
- War: the best motivation so far for investing in situational awareness of critical infrastructure

CAIDA: background & history

- Since 1997: narrowing the gap between Internet operations and science in face of global privatization
- Largely US taxpayer funded (nsf, dhs), plus sponsors
- Seek, analyze, communicate salient features of best available data on the Internet
- Use this data to prepare for the future
- Recent expansion of research agenda into policy and economics

CAIDA activities

- data sharing & curation for reproducible research (datcat, predict, ditl, commons)
- passive measurement: software, hardware, analysis
- dns traffic and vulnerability analyses
- active measurement, curation, analyses, modeling, simulation
- forward-looking: routing architecture for 1B nodes
- policy guidance: “top10 list”, IPv6 surveys, blog

Ten Things the FCC Should Know about the Internet

#1 Updating legal frameworks

- Updating legal frameworks to accommodate technological advancement of communications capabilities requires first updating other legal frameworks to accommodate empirically grounded research into what we have built, how it is used, and what it costs to sustain.

Where is the science (plan)?

#1 Updating legal frameworks

no aphorism is more frequently repeated...
than that we must ask Nature few questions, or ideally, one question at a time. The writer is convinced that this view is wholly mistaken.
Nature, he suggests, will best respond to a logically and carefully thought out questionnaire; indeed if we ask her a single question, she will often refuse to answer until some other topic has been discussed."

Sir Ronald A. Fisher, Perspectives in Medicine and Biology, 1973.

#2 Obstacles to progress

- Unfortunately for -- and due to -- well-intentioned policymakers, our scientific knowledge about the Internet is weak because researchers are typically not allowed access to any data on operational network infrastructure for reasons of economics, ownership, and trust (EOT).

Financial sector transparent in comparison..

#3 Available data a dire picture

- Despite the methodological limitations of Internet science today, the few data points available suggest a dire picture.

--Running out of addresses
--Scalability limits of routing system
--Pervasive peer-to-peer architectures incongruent with economic models
--Security and stability of naming, addressing, routing

#4 The problem is not so new

- This data access problem was recognized long ago for its detrimental impact on infrastructure protection capabilities; many public and private sector efforts have failed to solve it.

NSF, DHS, ISACs. & RIAA, MPAA.

#5 An absurd situation

- Public policy intended to protect individual user privacy places the research community in the absurd situation of not being able to do the most basic network research even on the networks established explicitly to support academic network research.

--> contradictory research on most fundamental issues with no way to validate/resolve.

#6 How data *is* being used

- While the looming problems of the Internet overwhelmingly indicate the need for a closer objective look, people with measurement capability on publicly accessible network infrastructure today are incented to infer as much private information on individual users as possible -- whether it's to target terrorists or ads

Only the neutral are forbidden

#7 Normal regulatory responses doomed

- The traditional mode of getting data from public infrastructures to inform policymaking – regulating its collection – is a quixotic path, since the government regulatory agencies have as much reason to be reluctant as providers regarding disclosure of how the Internet is engineered, used, and financed.

Tip of the iceberg intimidating.
Incentive and capital mis-aligned.

#8 Problematic responses

- The opaqueness of the infrastructure to empirical analysis has generated many problematic responses from rigidly circumscribed communities earnestly trying to get their jobs done.

Ipv6, address markets, NN, I2/NLR/GENI, PREDICT, researchers, FCC, bit movers.

#9 The news is not all bad

- The Internet's practical promise for individual freedom, democratic engagement, and economic empowerment, is sufficient inspiration for an open, technically literate conversation about how to invest in technologies and policies to support articulated social objectives.

How we got here matters

historical context

1966: Larry Roberts, “Towards a Cooperative Network of Time-Shared Computers” (first ARPANET plan)
(*we are still using the same stuff*)

1969: ARPANET commissioned by DoD for research

1977: Kleinrock’s paper “Hierarchical Routing for large networks; performance evaluation and optimization”
(we are still using the same stuff)

1980: ARPANET grinds to complete halt due to (statusmsg) virus

1986: NSFNET backbone, 56Kbps. NSF-funded regionals.
IETF, IRTF. MX records (NAT for mail)

1991: CIX, NSFNET upgrades to T3, allows .com. web. PGP.

1995: under pressure from USG, NSF transitions backbone to competitive market. no consideration of economics or security.

2005: *Economist* cover: “*How the Internet killed the phone business*” (Sept)

#10 Solutions will cross boundaries

- Even in the dim light we can ascertain some concrete constraints on the possible range of policy solutions, which all cross policy-technology boundaries and involve increasing the congruity between what we legislate and what we know.

Security, scalability, sustainability, stewardship

#10 Solutions will cross boundaries

- Catalog successes: web, voip, linux, wikipedia, ebay, blogosphere, social networks
- Catalog failures: ATM, interdomain multicast/QOS, routing security, Ipv6, DNSSEC

What attributes are unique to each

#10 Solutions will cross boundaries

- insecure software ecosystem
- unscalable routing/addressing architecture
- unsustainable cost structures
- broken stewardship models

What we believe about the infrastructure matters..

http://www.caida.org/

References

- Ten Things Lawyers Should Know About the Internet
  http://www.caida.org/publications/papers/2008/lawyers_top_ten/

kc@caida.org