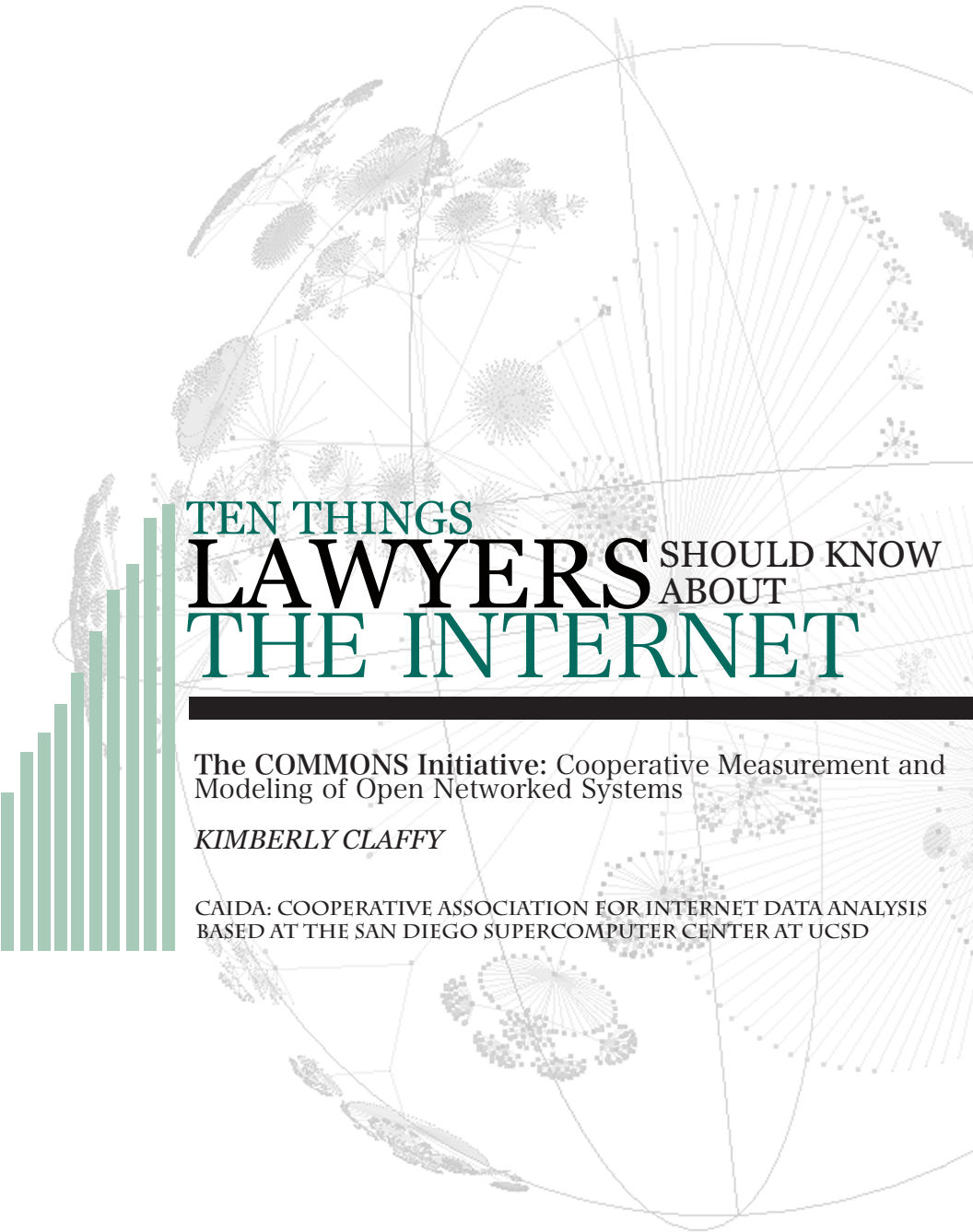


TEN THINGS LAWYERS SHOULD KNOW ABOUT THE INTERNET

The COMMONS Initiative: Cooperative Measurement and Modeling of Open Networked Systems

KIMBERLY CLAFFY

CAIDA: COOPERATIVE ASSOCIATION FOR INTERNET DATA ANALYSIS
BASED AT THE SAN DIEGO SUPERCOMPUTER CENTER AT UCSD

table of contents

about the author

Kimberly Claffy *received her Ph. D. in Computer Science from UCSD. She is Director and a principal investigator for CAIDA, and an Adjunct Professor of Computer Science and Engineering at UCSD. Kimberly's research interests include Internet measurements, data analysis and visualization, particularly with respect to cooperation and sharing of Internet data. She advocates the use of quantitative analysis to objectively inform public Internet policy discussions. Her email is* ***kc@caida.org.***

Adapted from:

http://www.caida.org/publications/papers/2008/10_things_Lawyers_Should_Know_About_The_Internet

Last year Kevin Werbach[1] invited me to his Supernova 2007[2] conference to give a 15-minute vignette on the challenge of getting empirical data to inform telecom policy. They posted the video of my talk[3] last year, and my favorite tech podcast ITConversations[4], posted the mp3[5] as an episode last week. I clearly needed more than 15 minutes...

In response to my "impassioned plea", I was invited to attend a meeting in March 2008 hosted by Google and Stanford Law School — Legal Futures[6] — a "conversation between some of the world's leading thinkers about the future of privacy, intellectual property, competition, innovation, globalization, and other areas of the law undergoing rapid change due to technological advancement." There I had 5 minutes to convey the most important data points I knew about the Internet to lawyers thinking about how to update legal frameworks to best accommodate information technologies in the 21st century. With a few more months of thought, here is my current top ten list of the most important things lawyers need to understand about the Internet.

1 **Kevin Werback bio**, http://werbach.com/about.html
2 **Supernova 07 Conference archive**, http://conversationhub.com/category/supernova07/
3 **"Closing the Interactive Loop"**, http://conversationhub.com/category/supernova07/
4 **ITConversations**, http://itc.conversationsnetwork.org/
5 **"No Access To Internet Data", Jun 2007**, http://itc.conversationsnetwork.org/shows/detail3440.html
6 **Legal Futures Conference**, **Mar 2008**, http://www.law.stanford.edu/calendar/details/1594/
7 **Creative Commons Attribution-No Derivative 3.0**, **2008**, http://creativecommons.org/licenses/by-nd/3.0/

point one

I. Updating legal frameworks to accommodate technological advancement 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.

There is increasing recognition that various legal frameworks (from copyright to privacy to wiretapping to common carriage) need updating in light of technological developments of the last few decades. Unfortunately, the light is too dim to really understand Internet behavior, usage patterns, architectural limitations, and economic constraints, because current legal frameworks for network provisioning also *prevent sharing of data with researchers*[8] to scientifically investigate any of these questions. Even for data that is legal to share, there are overwhelming counter incentives to sharing any data at all in the competitive environment we have chosen — *although not achieved*[9] — for the network provisioning industry.

So while I support updating legal frameworks to be congruent with reality, I think we need to first confront that we have no basis for claiming what reality is yet.

"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.*

point two

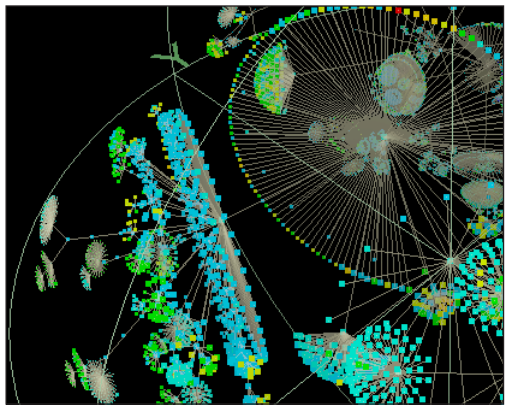
II. Our scientific knowledge about the Internet is weak, and the obstacles to progress are primarily issues of economics, ownership, and trust (EOT), rather than technical.

Economically, network research is perpetually behind network evolution — basic instrumentation can increase in cost 10X with one network upgrade, while network research budgets are lucky to stay even. But the ownership and trust obstacles are even greater: policy support for scientific Internet research has *deteriorated along several dimensions*[10] since the *National Science Foundation left the scene in 1995*[11], and further when *DARPA pulled out of funding academic networking research after 9/11*[12]. Some data points exposing the state of "Internet science":

A. Two decades of Internet research have failed to produce generally usable tools for bandwidth estimation, traffic modeling, usage characterization, traffic matrix estimation, topology mapping, or realistic Internet simulation, with progress primarily blocked on the ability to test them out in realistic network and traffic scenarios. A few researchers who do manage to get data via relationships of mutual trust (including CAIDA) are not allowed to share data with other researchers, inhibiting reproducibility of any result. Compared to established fields of science, it is hard to defend what happens in the field of Internet research as science at all.

B. U.S. (and other) government agencies continue to spend hundreds of millions of dollars per year on network research — with cyber security research being the most fashionable this decade — funding researchers who almost never have any data from realistic operational networks. An illustrative example: the National Science Foundation's *program for Internet security research*[13] spends ~$35M/year on dozens of research projects, none of which have data from operational Internet infrastructure.

C. Not only is traffic data off limits, but sharing data on the structure of the network is forbidden too — commercial ISPs are typically not even allowed to disclose the existence of peering agreements, much less their terms. So when developing tools for accurate Internet mapping, researchers cannot validate the connectivity inferences they make, since the information is typically intended to be secret.



D. OECD published a 53-page report: *Measuring security and trust in the online environment: a view using official data*[14]. As you may have guessed by now, the report about 'measuring security' is based on no measurements from any networks, only survey data reflecting user perceptions of their own security, which *other studies*[15] have shown to be uncorrelated with reality.

Another caveat: most security-related studies are published or funded by companies trying to sell more security software, their objectivity is also in dispute. Again, EOT factors render truth elusive.

point three

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

A. We're running out of IPv4 addresses that can be allocated (there are *many allocated addresses*[16] that are *not in observed use*[17] , but there is *no policy support (yet) for reclamation or reuse*)[18], and the purported technology solution (*IPv6*[19]) requires investment that *most ISPs are not prepared to make*[20]. Regardless of whether Internet growth is supported by IPv6 or a concerted effort to scrape more lifetime out of the current IPv4 protocol, it will induce growth of core Internet routing tables relying on a routing system that is increasingly inappropriate for the Internet's evolving structure. So while *it's fair to say that we need a new routing system*[21], no institution or agency has responsibility for developing one much less the global economic and political challenge of deploying it.

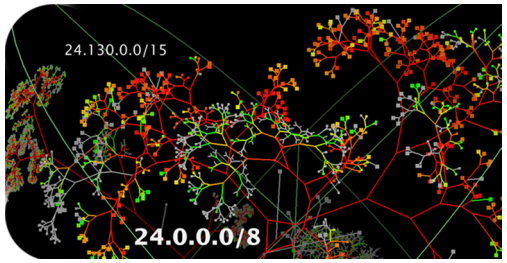
B. Pervasively distributed end-to-end peering to exchange information is not only threatening the integrity of the routing system, *but also the business models of the ISPs*[22]. Although it bears

8 **"Toward a Culture of Cybersecurity Research", 2008**, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1113014
9 **Telecommunications Act of 1996**, http://www.cybertelecom.org/notes/telecomact.htm
10 **"Measuring the Internet", Jan 2001,** http://www.caida.org/publications/papers/2000/ieee0001/
11 **"Post-NSFNET statistics collection"**, http://www.caida.org/publications/papers/1995/pnsc/
12 **"CS profs and the DOD", Sep 2007**, http://www.cra.org/govaffairs/blog/archives/000624.html
13 **NSF Trusted Computing program**, http://www.nsf.gov/funding/pgm_summ.jsp?pims_id=503326&org=NSF
14 **Measuring Security and Trust in the Online Environment**, **Jan 2008**, http://www.oecd.org/dataoecd/47/18/40009578.pdf
15 **McAfee/NCSA Cyber Security Survey, Oct 2007**, http://download.mcafee.com/products/manuals/en-us/McAfeeNCSA_Analysis09-25-07.pdf
16 **ANT Censuses of the Internet Address Space**, **Jun 2008**, http://www.isi.edu/ant/address/
17 **Mapping The IPV4 Address Space**, **Mar 2008**, http://maps.measurement-factory.com/
18 **ARIN's Number Resource Policy Manual**, **Aug 2008**, http://www.arin.net/policy/nrpm.html#eight1
19 **ARIN IPv6 Wiki**, http://www.getipv6.info/index.php/Main_Page
20 **ARIN & CAIDA IPv6 Survey Results**, **Apr 2008**, http://www.arin.net/meetings/minutes/ARIN_XXI/PDF/monday/IPv6_Survey_KC.pdf
21 http://blog.caida.org/best_available_data/2007/08/08/it-is-fair-to-say-that-we-need-a-new-routing-system/
22 **Jan 2008**, http://www.geek.com/time-warner-cable-to-experiment-with-internet-access-charges/

noting that the business models for moving Internet traffic around have long been suspect, since the network infrastructure companies that have survived the bubble have done so by spending the last fifteen years *manipulating*[23] the *network architecture*[24] and the *regulatory architecture*[25] away from the Internet architecture (smart endpoints) toward something they can control (smart network) in order to more *effectively monetize their assets*[26]. Since the Internet architecture was originally designed to be a *government-sponsored file-sharing network*[27] with no support for usage-based (or any) billing, its *failure as a platform for a purely competitive telecommunication industry*[28] is not surprising. But we are going to be so surprised.

C. There are demonstrated vulnerabilities in the most fundamental layers of the infrastructure (*naming*[29] and *routing*[30]) for which *technological*[31] *solutions*[32] have been developed but have failed to gain traction under the *political*[33] and *economic constraints*[34] of real-world deployment In the meantime, *over 98% of traffic sent to root domain name servers is pollution*[35].

D. The common lawyerly assumption that "the Internet security situation must not be so bad because the network is still pretty much working" discounts the fact that criminals using the Internet need it to work just as well as the rest of us. Although we *admit we don't know how to measure the exact size of botnets*[36] what we know for sure is that *millions of compromised (Windows) systems*[37] are taking advantage of network and host software vulnerabilities to support unknown (but underground estimates are many) billions of dollars per year of criminal activities (or activities that would be criminal if lawmakers understood enough to legislate against them) with no incentive framework to support their recovery. Although ICANN is trying to set policies to *counter some of the malfeasance*[38] that arguably falls under its purview (domain names and IP addresses), ICANN *lacks the architecture and legitimacy it needs to enforce any regulations*[39], and continues to struggle more than succeed at its own *mission*[40].



We don't have a lot of data about the Internet, but what little we have is unequivocally cause for concern.

point four

IV. The data dearth is not a new problem in the field; many public and private sector efforts have tried and failed to solve it.

A. Information Sharing and Analysis Centers, such as those that exist for the *financial services industry*[41] have been *attempted*[42] several times, but there is no research activity or channel to share data with the research community, nor any independent analysis of the performance or progress of such a group.

B. The National Science Foundation has spent at least $1M on CAIDA's *Internet measurement data catalog*[43] to support sharing of Internet measurements, but as a science and engineering funding agency, NSF could only fund the technical aspects of the data sharing activity: *developing a database*[44] to support curation, indexing, and annotation of Internet data collected by researchers and providers. Since the real obstacles have to do with economic, ownership (legal), and trust (privacy) constraints rather than technology issues, this catalog has been *less utilized*[45] than we hoped.

C. Recognizing that the *data sharing problem constitutes a threat to national security*[46] the U.S. Department of Homeland Security (specifically, *HSARPA*[47]) has spent 4 years developing a project — *PREDICT*[48]— to facilitate protected sharing of realistic network data that will enable cybersecurity researchers to validate the network security research and technologies they develop. Unfortunately after four years the PREDICT project has not yet launched, and when it does it will not be able to include data on networks *that serve the public*[49], since the legal territory is too muddy for DHS lawyers to navigate while *EFF lawsuits*[50] have everyone in the U.S. government skittish about acknowledging surveillance of any kind. Even the private networks that PREDICT can serve immediately, such as *Internet2*[51] (the research backbone in the U.S. *serving a few hundred*[52] educational, commercial, government, and international partners) have lamented that the PREDICT framework does not solve their two biggest problems: sketchy legal territory, and fear of RIAA subpoenas and/or lawsuits. Meanwhile, *other accounts*[53] (from *non-objective parties*[54], with no data sources) claim that

23 **Telecommunications Act of 1996**, http://www.cybertelecom.org/notes/telecomact.htm
24 **"The Walled Garden: Access To Internet and Digital Computer Communications Technology", Apr 1996**, http://homepages.ed.ac.uk/ajwil/disa.html
25 **Telecommunications Act of 1996**, http://www.fcc.gov/telecom.html
26 **IMS 'Reality Check'**, http://ims-insider.blogspot.com/2006/04/ims-reality-check.html
27 http://en.wikipedia.org/wiki/Arpanet
28 **"Consolidation Leads to ISP Shake-Out in Europe", Jul 2001**, http://www.thewhir.com/features/consolidation.cfm
29 **Oct 2006**, http://www.ripe.net/ripe/meetings/ripe-53/presentations/whats_wrong_with_dns.pdf
30 **"Tubular Routing", Mar 2008**, http://www.potaroo.net/ispcol/2008-03/routehack.html
31 **Domain Name System Security Extensions**, http://en.wikipedia.org/wiki/DNSSEC
32 **Secure BGP Project (S-BGP)**, http://www.ir.bbn.com/sbgp/
33 **"DNSSEC-The Opinion"**, http://ispcolumn.isoc.org/2006-10/dnssec3.html
34 **"Operational Requirements for Secured BGP"**, http://www.cs.columbia.edu/~smb/talks/dhs-routing.pdf
35 **Comparison of Traffic from DNS Root Nameservers in DITL 2006 and 2007**, http://www.caida.org/research/dns/roottraffic/comparison06_07.xml#concl
36 **Kanich, et al., "The Heisenbot Uncertainty Problem: Challenges in Separating Bots from Chaff"**, http://www.cs.ucsd.edu/~voelker/pubs/heisenbot-leet08.pdf
37 http://en.wikipedia.org/wiki/Botnets#References
38 http://www.icann.org/public_comment/#domain-tasting
39 **"ICANN Reform: Establishing the Rule of Law", Nov 2005**, http://www.prism.gatech.edu/%7Ehk28/ICANN_Rule-of-Law.pdf
40 **Feb 2008**, http://www.icann.org/general/bylaws.htm#I
41 **Financial Services-Information Sharing and Analysis Center**, http://fsisac.com/
42 **Information Sharing and Analysis Center (ISAC)**, **Jan 2001**, http://www.ntia.doc.gov/ntiahome/press/2001/itsac011601.htm
43 **"Correlating Heterogeneous Measurement Data to Achieve System-Level: Analysis of Internet Traffic Trends", Aug 2001**, http://www.caida.org/funding/trends/
44 **DatCat, indexed Internet measurement data**, http://www.datcat.org/
45 **DatCat traffic summary, Aug 2008**, http://imdc.datcat.org/stats/index.html
46 http://blog.caida.org/best_available_data/2008/03/25/we-should-be-able-to-do-a-much-better-job-at-modeling-internet-attacks/
47 http://en.wikipedia.org/wiki/Homeland_Security_Advanced_Research_Projects_Agency
48 **Protected Repository for the Defense of Infrastructure Against Cyber Threats (PREDICT)**, https://www.predict.org/
49 **Privacy Impact Assessment for PREDICT, Feb 2008**, http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_st_predict.pdf
50 **NSA Spying, cases and resources**, http://www.eff.org/issues/nsa-spying
51 http://www.internet2.edu
52 **Internet 2 Members list, Jul 2008**, http://www.internet2.edu/resources/Internet2MembersList.PDF
53 **"Comments of NBC Universal, Inc., to the Federal Communications Commission"**, http://www.publicknowledge.org/pdf/nbc-fcc-noi-20070615.pdf
54 **"The Movie Industry's 200% Error"**, http://insidehighered.com/views/2008/01/29/green

the vast majority of traffic on the Internet is *illegal by current laws*[55] and *ISPs should be held accountable*[56] for *preventing this traffic*[57]. Given the exposure to copyright lawsuits for file-sharing (ironically, what the Internet was *originally designed*[58] to do), the counter incentives to sharing data on operational networks grow stronger by the day.

point five

V. Thus the research community is 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.

This inability to do research on our own research networks leads to contradictions in our field of "science" that cannot be resolved, including on the most politically relevant network research questions of the decade: what are the costs and benefits of using QOS to support multiple service classes, to users as well as providers, and how should these service classes be determined? Two research papers on this same topic contradict each other — *Why Premium IP Service Has Not Deployed (and Probably Never Will*[59]) from *Internet2*[60] (the U.S. research and education backbone) and *The Evolving Internet - Traffic, Engineering, and Roles*[61] from ATT — with neither paper offering actual network data, although the Internet2 paper claims to be based on data from the Internet2 backbone. The ATT paper uses unsubstantiated numbers from invalidated sources on the web and a model and simulation construction with parameters arranged to prove the need for the kind of traffic management behavior that ATT lobbyists are trying to justify to regulators and their customers. As with many other questions about network architecture, behavior, and usage, there are valid (i.e., empirically validated) inferences to make regarding QoS versus the alternatives, which could immediately inform telecom and media policy, but researchers are not in a position to make them.

point six

VI. While the *looming problems of the Internet*[62] indicate the need for a closer objective look, a growing number of segments of society have network measurement access to, and use, private network information on individuals for purposes we might not approve of if we knew how the data was being used.

To the extent that we are investing public or private sector dollars in trying to measure the Internet, they are not in pursuit of answers to questions related to the overall network infrastructure's health, system efficiency or end-to-end performance, or any of the questions that engineers would recommend knowing about a communications system. The measurements happening today are either for *national security*[63] or *business purposes*[64], which both have an incentive to *maximize the amount of personal information they extract*[65] from the data. No one is investing in technology to learn about networks while minimizing the amount of privacy compromised in the process. This inherent *information asymmetry*[66] of the industry is at the root of our *inability to verify claims*[67] regarding either *security*[68] or *bandwidth crises*[69] justifying *controversial business practices*[70] that threaten an admittedly fuzzy, but *increasingly popular*[71] concept of *Internet access rights*.[72] Although the little data that *researchers can scrape together*[73], most of it from outside the U.S., do not support the "*p2p is causing a bandwidth problem*[74]" claim, the *press releases*[75] we see as a *popular*[76] *substitute for real data*[77] in the U.S. do support the claim that the current *Internet transit business model is broken*[78]. Whether the growth in traffic is due to http transport of *user-generated video*[79], or *radically distributed*[80] peer-to-peer file sharing (also *often video*[81]), there is *strong evidence*[82] from *network providers themselves*[83] that the *majority of bytes*[84] on the network are *people moving files*[85] from machine to machine, often the same files moving from a few sources to many users. Unfortunately, this evidence implies that the current network and policy architectures are *astonishingly inefficient*[86], and that *clean slate*[87] *Internet researchers*[88] should be thinking about

55 **"Home Copying - burnt into teenage psyche", Apr 2009**, http://www.guardian.co.uk/technology/2008/apr/07/digitalmusic.drm
56 **"IFPI hails court ruling that ISPs must stop copyright piracy on their networks"**, http://www.ifpi.org/content/section_news/20070704b.html
57 "**AT&T and Other I.S.P.'s May Be Getting Ready to Filter for copyrighted content at the network level"**, http://bits.blogs.nytimes.com/2008/01/08/att-and-other-isps-may-be-getting-ready-to-filter/index.html
58 http://en.wikipedia.org/wiki/Arpanet
59 **"Why Premium IP Service Has Not Deployed (and Probably Never Will)"**, http://qos.internet2.edu/wg/documents-informational/20020503-premium-problems-non-architectural.html
60 http://www.internet2.edu/
61 **"The Evolving Internet - Traffic, Engineering, and Roles"**, http://web.si.umich.edu/tprc/papers/2007/786/Evolving%20Internet.pdf
62 **"Top problems of the Internet and what can be done to help"**, http://www.caida.org/publications/presentations/2005/topproblemsnet/
63 **"Bush Order Expands Network Monitoring", Jan 2008**, http://www.washingtonpost.com/wp-dyn/content/article/2008/01/25/AR2008012503261.html?hpid=moreheadlines
64 **"Should AT&T police the Internet", Jan 2008**, http://news.cnet.com/Should-ATT-police-the-Internet/2100-1034_3-6226523.html?part=rss&tag=2547-1_3-0-20&subj=news
65 **Make extra money with a Google search box**, http://www.google.com/services/adsense_tour/page6.html
66 http://en.wikipedia.org/wiki/Information_asymmetry
67 **"Threats to the Internet: Too Much or Too Little Growth", Feb 2008**, http://www.internetevolution.com/author.asp?section_id=592&doc_id=146747
68 **"Cybersecurity measure unduly secretive"**, http://www.usatoday.com/tech/news/techpolicy/2002-07-25-cybersecurity-backlash_x.htm
69 **"Does Bell Really Have a P2P Bandwidth Problem?", Apr 2008**, http://www.circleid.com/posts/841710_bell_p2p_bandwidth_problem/
70 **"Comcast opens up about how it manages traffic"**, http://www.usatoday.com/printedition/money/20080421/nightmareside.art.htm
71 **The internet freedom fight goes to Washington**. http://www.savetheinternet.com/
72 **"Bill of Internet Access Rights", Jun 2006**, http://www.isi.edu/touch/internet-rights/
73 **A Day In The Life of the Internet: A Summary of the January 9-10, 2007 Collection Event**, http://www.caida.org/projects/ditl/summary-2007-01/#participants
74 *See footnote 69*
75 **Minnesota Internet Traffic Studies (MINTS), 2002**, http://www.dtc.umn.edu/mints/ispreports.html
76 **"Unleashed the 'Exaflood", Feb 2008**, http://online.wsj.com/article_email/SB120363940 010084479-lMyQjAxMDI4MDIzMjYyMzI5Wj.html
77 **Internet Study 2007: The Impact of P2P File Sharing, Voice over IP, Skype, Joost, Instant Messaging, One-Click Hosting and Media Streaming such as YouTube on the Internet**, http://www.ipoque.com/news_&_events/internet_studies/internet_study_2007
78 **"Avoiding Net traffic tie-ups could cost you in the future"**, http://www.usatoday.com/printedition/money/20080421/network_nightmarecov.art.htm
79 **Youtube,** http://www.youtube.com/
80 http://www.p2pfoundation.net/P2P_Computing
81 http://torrentfreak.com/japanese-file-sharing-population-explodes-071221/
82 **"Comments of AT&T on petitions of Free Press, Vuze, et al.. before the Federal Communications Committee in the matter of broadband industry practices", Feb 2008**, http://gullfoss2.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=6519841106
83 **"Comments of Verizon before the FCC in the matter of broadband industry practices", Feb 2008**, http://gullfoss2.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=6519841190
84 **"Comments of Comcast Corporation before the FCC in the matter of broadband industry practices", Feb 2008**, http://gullfoss2.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=6519840991
85 **"Comments of Time Warner Cable Inc., before the FCC in matters of broadband industry practices", Feb 2008**, http://gullfoss2.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=6519841176
86 **"Democracy Now! Saves $1,000 a month with bittorrent", Feb 2008**, http://www.getmiro.com/blog/2008/02/huge-cost-savings-bittorrent-vs-http/
87 http://cleanslate.stanford.edu/
88 **FIND (Future Internet Design),** NSF research program whose goal is to consider requirements for a global network of 15 years from now, and how we would build such a network if we could design it from scratch, http://www.nets-find.net/

how to create *truly scalable*[89] *inter-domain routing*[90] and *policy architectures*[91] that are *content-centric*[92], leverage our best understanding of the *structure of complex networks*[93], and still manage to *respect privacy*[94]. No easy trick, especially with no viable deployment path for such a new architecture, at least in the U.S. where we have *jettisoned the policy framework*[95] that *allowed innovations*[96] like the Internet. It should be no surprise if the *status quo is unsustainable*[97], since we are *using the network quite differently*[98] from *how it was intended*[99]. But if a new network architecture is needed, that's a discussion that needs to include some validated empirical analysis of

what we have already built. So long as the network infrastructure companies are so *counterincented to share data*[100], we will continue having to make trillion-dollar communication and technology policy decisions in the dark.

point seven

VII. The traditional mode of getting data from public infrastructures to inform policymaking — regulating its collection — is a quixotic path, since the *government regulatory agencies*[101] have as much *reason to be reluctant*[102] as *providers*[103] regarding disclosure of how the Internet is engineered, used, and financed.

For every other critical infrastructure in society we have devoted a government agency to its stewardship. The Internet was designed for a *cooperative*[104] rather than competitive policy architecture, so its designers did not consider regulatory aspects. But as a communications infrastructure serving the public, most regulatory aspects of Internet fall under the jurisdiction of the agency who regulates the *tubes*[105] it typically runs atop: in the United States that means the FCC. Unfortunately, the FCC is not completely *up to speed*[106] on the Internet, and does not even approve of how it is *measuring broadband penetration*[107]. The FCC has no empirical basis in fact nor apparent *authority*[108] in a conversation about traffic, structure, pricing, or vulnerabilities on the network since it has no access to data from Internet infrastructure beyond what providers volunteer to provide. And yet *little data*[109] is needed to reveal that the Internet's underlying network architecture, implementation, and usage is fundamentally inconsistent with almost every aspect of our current communications and media policy architecture. The Internet sheds deep skepticism on current legal frameworks for copyright, wiretapping, and privacy, as well as transforms or destroys dozens of industries that hold great economic and political power today.

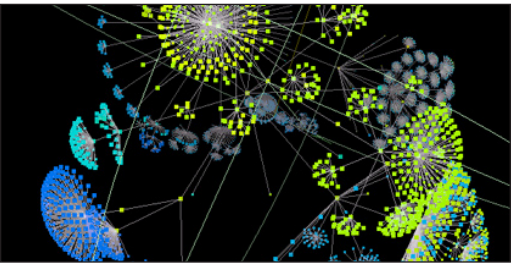
The national security components of Internet regulation, from *wiretapping*[110] to *disaster recovery*[111] to *unstable*[112] *leadership*[113] *lamenting its budgetary and policy handicaps*,[114] inspire *concern*[115] than hope. That over 1% of observed web pages are *modified in flight without our knowledge*[116] is *no source of comfort*[117] either.

Hence it should be no surprise if solutions to measurement, like other *persistent problems of the Internet*[118], require engaging deeply with economics, ownership and trust issues. Alas, Internet economics research is one of the few fields *worse off*[119] than Internet traffic or topology research with regard to the ability to validate any models or assumptions. (If you think tcpdump and traceroute are replete with measurement error, you should try analyzing the economics of network infrastructure companies. And if you think packet header and internal topology data is hard to get, you should try to get financial numbers from the same companies broken out by service offered so you could see how the *ec-*

89 **"On Compact Routing for the Internet"**, http://www.caida.org/publications/papers/2007/compact_routing/
90 **Routing Research Group,** http://www.irtf.org/charter?gtype=rg&group=rrg
91 **"Retrograde Inversion", Apr 2008**, http://scrawford.net/blog/retrograde-inversion/1148/
92 http://en.wikipedia.org/wiki/Content-centric_networking
93 **"Self-similarity of complex networks and hidden metric spaces"**, http://www.caida.org/publications/papers/2008/self_similarity/
94 **Electronic Privacy Information Center**, http://epic.org/
95 **National Cable & Telecommunications Association et al. v. Brand X Internet Services et al., 2005**, http://www.law.cornell.edu/supct/html/04-277.ZS.html
96 **Common Carriers**, http://www.cybertelecom.org/notes/common_carrier.htm
97 **"PNSol: Answer to the broadband riddle?"**, http://www.telco2.net/blog/2008/04/post_13.html
98 **PEW /Internet Reports: Online Activities**, http://www.pewinternet.org/PPF/c/1/topics.asp
99 **Inventing the Internet, Jul 2000,** http://www.amazon.com/Inventing-Internet-Inside-Technology-Abbate/dp/0262511150/
100 *See footnote 8*
101 **Bureaucracy: What Government Agencies Do And Why They Do It, Jan 1991**, http://www.amazon.com/Bureaucracy-Government-Agencies-Basic-Classics/dp/0465007856/
102 **"Can the FCC Handle The Truth?", Apr 2008**, http://www.publicknowledge.org/node/1529
103 **"If Comcast Shares Broadband Deployment Data, The Terrorists Win", Mar 2008**, http://www.dslreports.com/shownews/If-Comcast-Shares-Broadband-Deployment-Data-The-Terrorists-Win-92408
104 **"Tward A Cooperative Network Of Time-Shared Computers", Nov 1966**, http://www.packet.cc/files/toward-coop-net.html
105 **Senator Ted Stevens talking about the Net Neutrality Bill: "Series of Tubes",** http://www.youtube.com/watch?v=f99PcP0aFNE
106 **"FCC to start collecting more detailed broadband info", Mar 2008**, http://www.rcrnews.com/apps/pbcs.dll/article?AID=/20080321/SUB/669906587/1005/allnews
107 http://blog.caida.org/best_available_data/2008/03/30/measuring-broadband-penetration/
108 **"Comcast: FCC lacks any authority to act on P2P blocking", Mar 2008**, http://arstechnica.com/news.ars/post/20080318-comcast-fcc-lacks-any-authority-to-act-on-p2p-blocking.html
109 *See point three*
110 **"Congress worries that .gov monitoring will spy on Americans", Feb 2008**, http://news.cnet.com/8301-10784_3-9882031-7.html
111 **"Internet Infrastructure: Challenges in Developing a Public/Private Recovery Plan", 2006**, http://www.gao.gov/cgi-bin/getrpt?GAO-06-1100T
112 **"Help (still) wanted: Cybersecurity czar", Jul 2006**, http://news.cnet.com/Help-still-wanted-Cybersecurity-czar/2100-7348_3-6094055.html
113 **"Cybersecurity czar will have hard road ahead", Jun 2005**, http://www.securityfocus.com/news/11194
114 **"RSA: Chertoff Likens U.S. Cyber Security to 'Manhattan Project'", Apr 2008**, http://www.informationweek.com/news/security/government/showArticle.jhtml?articleID=207100489
115 **"Will the next U.S. president lead on cybersecurity?", Oct 2007**, http://news.cnet.com/8301-10784_3-9807450-7.html
116 **"Detecting In-Flight Page Changes with Web Tripwires"**, http://www.usenix.org/events/nsdi08/tech/full_papers/reis/reis_html/index.html
117 **"The Digital Imprimatur: How big brother and big media can put the Internet genie back in the bottle", Sept 2003**, http://www.fourmilab.ch/documents/digital-imprimatur/
118 *See footnote 62*
119 http://blog.caida.org/best_available_data/2007/10/07/internet-infrastructure-economics-top-ten-things-i-have-learned-so-far/

omics are actually evolving[120].)

Unfortunately (again) understanding the economics of the system is not where spare private or public sector capital is going. In the 1990's the telecoms spent their capital *suing each other*[121] and *the government*[122] over *laws so vaguely written*[123] as to *defy consistent interpretation*[124], much less measurable enforcement, across any *two constituencies*[125] in the ecosystem. This decade we are spending our capital *suing the telecoms*[126] for not suing the government after 9/11 when the *government asked them to break laws*[127] that are



just as outdated as the copyright laws[128]. *Thomas Jefferson*[129] would no doubt *recommend rewriting all of it from scratch*[130]. Unfortunately the timing is bleak: these developments are occurring at a time when *sustaining Internet growth*[131](which, no, we still *do not have good ways to measure*[132]..) will require extraordinary investment of *capital, as well as realignment of incentives*[133] to promote cooperation among competitive players. Where does that capital and incentive to cooperate come from?

point eight

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

A. To its credit, the *IETF*[134] acknowledged and endeavored to solve the technical limitations of the current *IPv4 protocol*[135], primarily the *insufficient number of addresses*[136] and the *inherent scalability limitations of*[137] *the routing architecture*[138]. To its *chagrin*[139], the IETF learned that neither the *philospher king nor rough consensus-based*[140] approach would yield an architecture that made progress on both problems at the same time. So the IETF *punted on the routing problems*[141] since they seemed further away, and focused on building a new network architecture that had a larger number of addresses, and *some other*[142] stuff most people don't usually mention. But because today's addressing and routing architectures are *fundamentally related*[143] a larger number of addresses actually exacerbates the routing problem, getting us closer to the wall that seemed further away. In the meantime, the current IPv4 routing table is already splintering into smaller pieces as network operators engineer finer-grained control over traffic patterns. So, while IPv6 exists as a set of technologies, many experts are *grim about its future, since it doesn't solve*[144] the fundamental routing scalability problem.

B. Most *network operators*[145], especially for-profit ones, cannot justify the investment to deploy IPv6 when *their customers are not asking for it*[146], and their customers won't ask for it until they can no longer get IPv4 addresses. Large network operators continue to remind IETF engineers that they *didn't solve the problem the network operators really need solved*[147]. Operators do realize they are all in this together, but they aren't institutionally structured to think *longer than five years out*[148]. They also lack the capital, legal framework, and incentive to develop an alternative replacement, even in partnership with their suppliers. (The last time we *upgraded the network architecture*[149] the network was under the control of not only the U.S. government but the *U.S. military*[150]. And it still took a couple of rounds of threats to cut off funding to attached sites who did not upgrade!) Instead, operators are busy experimenting with business models to try to figure out how to make a profit on IP transit, e.g., *fancy QOS services that customers aren't asking for*[151], *metered pricing*[152] (known to *have its own problems*[153]), or giving up and *getting rid of the part of the company that moves IP traffic around*[154]. They have also recently experimented with *reforming their industry trade meetings*[155] to be more useful given that they aren't authorized to share any significant information about their own networks. In the meantime, if they have one, they heavly subsidize from the *magnificently profitable wireless*[156] side of the company while they build the case for more deregulation.

C. Thinking about the health of the Internet ten years out or longer should theoretically happen within the stewardship missions of *ICANN*[157] and the ICANN-rooted *address registries*[158], who lease Internet address space based on *demonstrated need*[159]. The ICANN and registry communit-

125 **Reciprocal Compensation**, http://www.cybertelecom.org/broadband/Rcomp.htm
126 http://www.eff.org/nsa
127 http://en.wikipedia.org/wiki/NSA_warrantless_surveillance_controversy
128 http://en.wikipedia.org/wiki/Foreign_Intelligence_Surveillance_Act_of_1978
129 **The Thomas Jefferson Hour**, http://www.jeffersonhour.org/
130 **Thomas Jefferson Hour episode: Constitutional Convention**, http://makochemedia.com/files/Show%20672%20Constitutional%20Convention.mp3
131 **"Eight Bold Steps To A National Broadband Strategy:", Jan 2007**, http://www.baller.com/pdfs/baller-lide_8Steps_NatBBStrategy.pdf
132 **"IPv6 Deployment: Just where are we?", Apr 2008**, http://www.potaroo.net/ispcol/2008-04/ipv6.html
133 **"CAIDA and ARIN Release IPv6 Survey", Apr 2008**, http://www.circleid.com/posts/84136_caida_arin_ipv6_survey/
134 **Internet Engineering Task Force**, http://www.ietf.org/overview.html
135 **Internet Protocol version 4 (IPv4)**, http://en.wikipedia.org/wiki/IPv4
136 **IPv4 exhaustion**, http://en.wikipedia.org/wiki/IPv4#Exhaustion
137 **"Models of policy based routing", Jun 1989**, http://www.faqs.org/rfcs/rfc1104.html
138 **NSFNET routing architecture, Feb 1989**, http://www.faqs.org/rfcs/rfc1093.html
139, 140 **Process for Organization of Internet Standards Working Group (POISED), Jun 1994**, http://www.apps.ietf.org/rfc/rfc1640.html
141 **"Lessons from IPv6"**, http://www.cs.columbia.edu/~smb/talks/ipv6-lessons.pdf
142 **Internet Protocol version 6 (IPv6)**, http://en.wikipedia.org/wiki/IPng
143 **"RFC4116 - IPv4 Multihoming Practices and Limitations", Jul 2005**, http://www.faqs.org/rfcs/rfc4116.html
144 **"Storm clouds looming for Internet, experts say", Apr 2008**, http://www.infoworld.com/article/08/04/17/Storm-clouds-looming-for-Internet-experts-say_2.html
145 **Nanog (North American Network Operators' Group)**, http://www.nanog.org/
146 **ARIN & CAIDA IPv6 Survey Results, Apr 2008**, http://www.arin.net/meetings/minutes/ARIN_XXI/PDF/monday/IPv6_Survey_KC.pdf
147 **"RFC4116 - IPv4 Multihoming Practices and Limitations", Jul 2005**, http://www.faqs.org/rfcs/rfc4116.html
148 **The Art of the Long View: Planning for the Future in an Uncertain World, 1991**, http://www.gbn.com/BookClubSelectionDisplayServlet.srv?si=361
149 http://en.wikipedia.org/wiki/Network_Control_Protocol
150 **U.S. Department of Defense**, http://www.defenselink.mil/
151 *See footnote 61*
152 **"Time Warner Cable to experiment with Internet access charges", Jan 2008**, http://www.geek.com/time-warner-cable-to-experiment-with-internet-access-charges/
153 **"Why Metered Broadband Slows Internet Innovation"**. http://www.techdirt.com/articles/20070911/194749.shtml
154 **"Time Warner to unplug cable business", Apr 2008**, http://www.ft.com/cms/s/0/42e6616a-16a7-11dd-bbfc-0000779fd2ac.html
155 **"NANOG Evolution-What's Next?"**, http://www.nanog.org/evolution.html
156 **"Led by Wireless Unit, AT& T Reports a 21.5% Gain", Apr 2008**, http://www.washingtonpost.com/wp-dyn/content/article/2008/04/22/AR2008042202921.html
157 *See footnote 40*
158 **The Address Supporting Organization**: http://aso.icann.org/about.html
159 **ARIN Number Resource Policy Manual,** http://www.arin.net/policy/nrpm.html

ies recognize the limitations of IPv6, and by now also the *limitations of the IETF*[160]. IETF experts are *similarly astute*[161] about the *problems with ICANN*[162]. And of course both communities are aware of the pressure on the current address space. Since IPv6 is the only existing solution, they both *promote IPv6 deployment*[163], although they *lack reliable methods*[164] to *measure IPv6 uptake*[165] without *data from operators*[166]. So, this year they are finally re-discussing a backup plan: *privatizing IPv4 address markets*[167], in case they *run out of IPv4 addresses*[168] before IPv6 gains traction. There is *little background*[169] *research on the implications*[170] of *private ownership of addresses*[171], but what exists is *not auspicious*[172]. Furthermore, the possibility that a legitimate market for IPv4 address may emerge will itself impede the uptake of IPv6, so the bottom-up registries are inherently conflicted regarding the problem they're trying to solve.

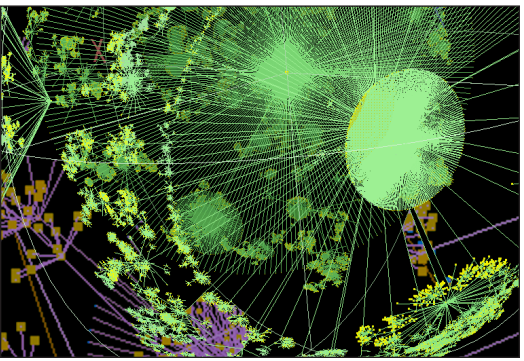
D. Meanwhile, over in the *media policy*[173], *reform*[174], *passionate activist*[175], and *well-intentioned legal scholar*[176] corner of cyberspace, it is as if *Eli Noam*[177]'s *warning about the imminent death of common carriage*[178] were not published fourteen years ago. Despite the *lack of any proposed operationally enforceable definition*[179] of network neutrality, the *conversation thrives*[180]— an understandable post-traumatic reaction to the recent jettison of at least *eight centuries of legal doctrine*[181] from our primary communications fabric. Even the FCC is *looking for ideas*[182] (strangely, they're *explicitly not interested in data*[183], despite *clear indications*[184] that *the free market evolution of IP economics*[185] is the *root cause*[186] of the mess.) When the dizziness subsides, we will have to acknowledge that the carriers are right: *it would be a disaster if the government told carriers how to manage congestion on their networks*[187], which is why the endgame must be — as it has always been with essential facilities and common carriage — that carriers do not have financial interest in the content of what they're carrying. But that idea — although it is the same type of structural regulation that made the Internet possible — offends any capitalist sense of profit margins.

E. Academic Internet researchers also operate in a *funding environment*[188] that does not promote *tackling 10-year problems*[189], nor are they equipped to navigate the conflict of interests between the university and the providers of network data. Providers either legally cannot or are reluctant to share data without restrictions on what can be published about their network, and universities have rules limiting such restrictions. And so federal agencies funding research continue to spend millions of R&D dollars per year developing *lots*[190] of *technology*[191], even *legal technology*[192] to promote *data retention*[193] and *sharing*[194], but the agencies and the taxpayers they represent get little in return. A related problem is that the lack of experience with data sharing in an admittedly quite young field of science means that there is no established *code-of-conduct*[195] for *protecting*[196] *user privacy*[197] and *engaging with Institutional Review Boards*[198] to navigate ethical issues in Internet measurement research. Worse yet, conservative interpretations of the current relevant statutes conclude that *most network measurement research is currently approximately illegal*[199], but there is no consensus on *what kind of legislative changes are needed*[200], if any. The stunted legal process prevents sharing of data sets that could help solve immediate problems, but the collateral damage is that it prevents informed discussion of what even needs to be known on the net, and who needs to know it. Do we want to know how much peer-to-peer traffic is transiting backbone links? How much encrypted traffic? How much copyrighted traffic? Right now there is insufficient access to data to any of

160 **"Into the Future with the Internet Vendor Task Force - A very Curmudgeonly View or Testing Spaghetti - a Wall's Point of View"**, http://rip.psg.com/~randy/051000.ccr-ivtf.html
161 **IETF (Internet Vendor Task Force) summary, Sep 2002**, http://www.ripe.net/ripe/meetings/ripe-43/presentations/ripe43-plenary-ietf-icann/sld022.html
162 **"An ICANN reform plan", Jun 2002**, http://www.alvestrand.no/icann/splitting.html
163 **ARIN IPv6 Wiki**, http://www.getipv6.info/index.php/Main_Page
164 See footnote 132
165 **IPv6 AS-level Topology 2008,** http://www.caida.org/research/topology/as_core_network/ipv6.xml
166 *See footnote 146*
167 **IPv4 Transfer Policy Proposal (2008-2)**, http://www.arin.net/policy/proposals/2008_2.html
168 **"The End of the (IPv4) World is Nigher! ", Jul 2007**, http://www.potaroo.net/ispcol/2007-07/v4end.html
169 **"RFC1744 - Observations on the Management of the Internet Address", Dec 1994**, http://www.faqs.org/rfcs/rfc1744.html
170 **"RFC 1744 and its discontents"**, http://lists.arin.net/pipermail/ppml/2008-April/010639.html
171 **"Financial Incentives for Route Aggregation and Efficient Address Utilization in the Internet", 1996**, http://www.cs.columbia.edu/~smb/papers/piara/Final.htm
172 **"'Address Ownership' Considered Fatal", Mar 1995**, ftp://ftp.ietf.org/ietf-online-proceedings/95apr/area.and.wg.reports/ops/cidrd/cidrd.rekhter.slides.ps
173 **Media Access Project**, http://www.mediaaccess.org/
174 **Free Press**, http://www.freepress.net/
175 http://www.savetheinternet.com/
176 **"Why You Should Care About Network Neutrality", May 2006**, http://www.slate.com/id/2140850/
177 **Eli M. Noam bio**, http://www.citi.columbia.edu/elinoam/
178 "**Beyond Liberalization II: The Impending Doom of Common Carriage", Mar 1994**, http://www.columbia.edu/dlc/wp/citi/citinoam11.html
179 **"OPINION: Would the real Network Neutrality please stand up?", Nov 2005**, http://www.telepocalypse.net/archives/000822.html
180 **"Net Neutrality's Quiet Crusader: Free Press's Ben Scott Faces Down Titans, Regulators in Battle Over Internet Control", Mar 2008**, http://www.washingtonpost.com/wp-dyn/content/article/2008/03/27/AR2008032703618.html?hpid=sec-business
181 http://www.isen.com/blog/2007/05/making-network-neutrality-sustainable.html
182 **"FCC seeks public comment on network neutrality", Jan 2008**, http://www.cedmagazine.com/FCC-seeks-public-comment-on-network-neutrality.aspx
183 **"FCC chief backs AT&T bid to waive cost data", Apr 2008**, http://www.reuters.com/article/governmentFilingsNews/idUSN2433101820080424?feedType=RSS&feedName=governmentFilingsNews&rpc=408
184 **"Telecom carriers: 'Phantom' voice traffic costing billions", Apr 2008**, http://www.infoworld.com/article/08/04/23/Telecom-carriers-Phantom-voice-traffic-costing-billions_1.html

185 **"The Evolution of U.S. Internet Peering Ecosystem", Nov 2003**, http://www.nanog.org/mtg-0405/pdf/norton.pdf
186 **"Where's the Money? - Internet Interconnection and Financial Settlements", Jan 2005**, http://isp-column.isoc.org/2005-01/interconns.html
187 **"My Interview in WorldChanging", Feb 2008**, http://www.isen.com/blog/2008/02/my-interview-in-worldchanging.html
188 **NITRD**, http://www.nitrd.gov/
189 *See footnote 148*
190 **DatCat, indexed Internet measurement data**, http://www.datcat.org/
191 **"The Devil and Packet Trace Anonymization"**, http://www.icir.org/enterprise-tracing/devil-ccr-jan06.pdf
192 *See footnote 48*
193 **The Datapository: A collaborative network data analysis and storage facility**, http://www.datapository.net/
194 **Deep Internet Performance Zoom (DipZoom)**, http://dipzoom.case.edu/
195 "**Issues and Etiquette Concerning Use of Shared Measurement Data"**, http://www.imconf.net/imc-2007/papers/imc80.pdf
196 **Data Sharing and Anonymization**, http://www.caida.org/data/anonymization/
197 **The 1st ACM Workshop on Network Data Anonymization, 2008**, http://www.ics.forth.gr/~antonat/nda08.html
198 **"IRBs and Security Research: Myths, Facts and Mission Creep", Mar 2008**, http://www.usenix.org/events/upsec08/tech/full_papers/garfinkel/garfinkel_html/
199 **"Legal Issues Surrounding Monitoring During Network Research (Invited Paper)"**, http://www.imconf.net/imc-2007/papers/imc152.pdf
200 *See footnote 8*

these questions. And answering them will come at a cost to the social contract of privacy. The conversation over how to make these trade-offs has *barely begun*[201]. For one, the academic community is too busy *fighting lawsuits*[202], the greatest incentive yet for universities to not retain data on network usage. So, while academic researchers do *generate*[203] *quite a bit*[204] of *intellectually meritorious*[205] *work*[206], they are forced to choose scientific problems based on what data they can manage to scrape together (bottom- up) rather than *picking the most important problems*[207] to study and getting the data needed to rigorously



study them. Recently, a group of well-respected academics have become sufficiently desperate at their inability to *study, modify, and share*[208] aspects of the Internet, that they've proposed *building their own sandbox*[209] to develop and test innovative network technologies. It's like network neutrality at the research layer, an apparently irresistible attempt to recover some *objectivity*[210] in the field, but in both cases *symptomatic*[211] of the *need for deeper inquiry*[212]

F. The (predominantly libertarian) engineers in the router trenches have self-organized into *squadrons of individual engineers*[213] and *analysts*[214]: skilled, bright, principled people who until recently mostly believed that if they worked hard enough, they could clean up the gutters of cyberspace without government intervention. Even these groups are now finally *acknowledging*[215] that without *better support for protected data-sharing*[216], *partnerships with government*[217], and more educated law construction and *enforcement*[218], even their best efforts plus the market *cannot fix*[219] the security problems. And although no one currently has positive expectations about the government doing any better anytime soon, neither are we in a position to claim the current lack of governance is working.

G. For the *U.S. regulatory agency*[220] *still reeling*[221] from the damage wrought by the *1996 (U.S. Telecom) act*[222] and its *lifetime employment for lawyers*[223], the opaqueness of the U.S. infrastructure, even to them, keeps them in the difficult position of trying to set policy in the dark. (Ironically the FCC us the agency who should lead solutions to this problem, but as mentioned, their behavior suggests they want *as little data as possible*[224], since they have already *made up their mind*[225] about how to (not) regulate the Internet.)

H. Innovative software developers *move away from more oppressive legal frameworks*[226], the net effect of which is to deprive the country of associated tax revenue and innovative climate.

I. Last but most important, the users, the youngest and most progressive of which are *embracing activity*[227] that is *arguably criminal*[228] under *current legal frameworks*[229]. Although it is well-established that supporting and enforcing these legal frameworks (a tax-funded activity whose costs are unknown) does great *economic damage*[230] while *sacrificing privacy and freedom*[231](not the best trade citizens have made), Hollywood insists (based on no verified data, natch), that on the contrary, it's the sharing of zero marginal cost goods that is causing the *economic damage*[232]. While some governments admit they have *no interest in tracking kids sharing music*[233], for-profit entities now forced to partner with content providers for economic reasons (since as we know by now, you *can't maximize profit just moving bits around*[234]) will find the *temptation*[235] *irresistible*[236].

All these communities have tremendous insights into pieces of the problem, all are filled with earnest people trying to do their job, constrained by their *institutional*[237] *context*[238]. But no one has oversight for *coordination or even articulation of the global picture*[239]. While the best available da-

202 **"Universities Baffled By Massive Surge In RIAA Copyright Notices", Apr 2008**, http://blog.wired.com/27bstroke6/2008/04/riaa-sends-spik.html
203 **ACM SIGCOMM 2008**, http://conferences.sigcomm.org/sigcomm/2008/
204 **Passive and Active Measurement Conference 2008**, http://pam2008.cs.wpi.edu/
205 **Internet Measurement Conference (IMC)**, http://www.imconf.net/
206 **IEEE/ACM Transactions on Networking**, http://www.ton.cs.umass.edu/
207 **"Richard Hamming 'You and Your Research'", Mar 1986**, http://magic.aladdin.cs.cmu.edu/wp-uploads/hamming.pdf
208 **Free Software Foundation**, http://www.fsf.org/
209 **Global Environment for Network Innovations**, http://www.geni.net/
210 **Objectivity, Oct 2007**, http://www.amazon.com/Objectivity-Lorraine-Daston/dp/1890951781/
211 **"Misuing Network Neutrality to Eliminate Common Carriage Threatens Free Speech and the Postal System", 2006**, http://www.ftc.gov/os/comments/broadbandwrkshop/527031-00066.pdf
212 http://blog.caida.org/best_available_data/2007/09/
213 **Castlecops**, http://www.castlecops.com/
214 **MAAW (Messaging Anti-abuse Working Group)**, http://www.maawg.org/about/
215 **"Law Enforcement Engagement & Incident Response Handling: NANOG Engagement", Feb 2008**, http://www.nanog.org/mtg-0802/presentations/Ferguson_Cyber_Crime.pdf
216 **Multi-State Information Sharing and Analysis Center**, http://www.msisac.org
217 **"Stopping Spam at its Source: Microsoft Partnered with Government and Law Enforcement in 003"**, http://www.microsoft.com/presspass/features/2004/feb04/02-10spamenforce.mspx
218 **NANOG mailing list: "Re: handling ddos attacks", May 2004**, http://www.irbs.net/internet/nanog/0405/0521.html
219 **"Information Security Economics - and Beyond", 2008**, http://www.cl.cam.ac.uk/~rja14/Papers/econ_czech.pdf
220 http://www.fcc.gov/
221 http://www.fcc.gov/telecom.html
222 http://www.ntia.doc.gov/top/publicationmedia/newsltr/telcom_act.htm
223 **"Untangling the Next Telecom Act", Mar 2006**, http://www.inthesetimes.com/article/2524/
224 **"FCC chief backs AT&T bid to waive cost data", Apr 2008**, http://www.reuters.com/article/governmentFilingsNews/idUSN2433101820080424?feedType=RSS&feedName=governmentFilingsNews&rpc=408
225 **Written statement of Kevin J. Martin before the U.S. Senate Committee on Commerce, Science and Transportation, Apr 2008**, http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-281690A1.pdf
226 **Testimony of Sam Yagan, Sep 2005**, http://judiciary.senate.gov/testimony.cfm?id=1624&wit_id=4689
227 **"Japanese File-Sharing Population Explodes", Dec 2007**, http://torrentfreak.com/japanese-file-sharing-population-explodes-071221/
228 **"95% of Kids Aged 18-24 Are Pirating Music", 2008**, http://gizmodo.com/377067/95-of-kids-aged-18+24-are-pirating-music
229 http://www.questioncopyright.org/
230 **"What's Wrong With Copy Protection", Feb 2001**, http://www.toad.com/gnu/whatswrong.html
231 **Digital Freedom**, http://digitalfreedom.org/utilities/2008/01/piracy-not-just-for-public-any-more.html
232 **"The True Cost of Motion Picture Piracy to the U.S. Economy", Sep 2006**, http://www.ipi.org/ipi%5CIPIPublications.nsf/PublicationLookupExecutiveSummary/A6EB1EAC4310AF6F862571F7007CB6AF
233 **"Anti file-sharing laws considered", Oct 2007**, http://news.bbc.co.uk/2/hi/technology/7059881.stm
234 **"Broadweave to heal iProvo by shedding wholesale fiber model", May 2008**, http://telephonyonline.com/fttp/news/broadweave-iprovo-wholesale-0507/
235 **"AT&T and Other I.S.P.'s May Be Getting Ready to Filter", Jan 2008**, http://bits.blogs.nytimes.com/2008/01/08/att-and-other-isps-may-be-getting-ready-to-filter/index.html
236 **"AT&T Pushes Internet Piracy Filters At CES", Jan 2008**, http://www.dslreports.com/shownews/ATT-Pushes-Internet-Piracy-Filters-At-CES-90827
237 *See footnote 101*
238 **Supercapitalism: The Transformation of Business, Democracy, and Everyday Life, Sep 2008**, http://www.amazon.com/Supercapitalism-Transformation-Business-Democracy-Everyday/dp/0307277992/
239 **"Why States Need an International Law for Information Operations", Jan 2008**, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1083889

ta makes it obvious that legal repair and renewal is crucial to democracy — communications technology being no exception — we are currently pursuing enlightened policy in the dark. Which begs the question: what is the most important ingredient to enlightened policy?

"Such is the irresistible nature of truth that all it asks, and all it wants, is the liberty of appearing." Thomas Paine (1737 - 1809)

point nine

IX. The news is not all bad: there is a reason everyone wants to be connected to all the world's knowledge — as well as each other — besides its status as the most powerful complex system ever created by man. The Internet's *practical promise*[240] for individual freedom, democratic engagement, and economic empowerment, is also unparalleled. This promise is sufficient inspiration for an open, technically literate conversation about how to invest in technologies and policies to support articulated social objectives.

A. David Clark's conclusion that the federally funded network research community's "*real accomplishment was not in computing but in connecting people*[241]" captures a century of thought. Although the openness of the architecture is the root of its many vulnerabilities, it was also the aspect that allowed enough self-organizing momentum to grow the network as *fast as it did*[242]. The results are *noisy*[243], the *journey messy*[244], the *future uncertain*[245], the *most pessimistic scenarios*[246] ominous. But the positive effects are also incalculable, particularly the potential for an unprecedented *increase in individual freedom*[247], the often de-emphasized, yet primary, social objective of both democracy and markets.

B. The *p2p file-sharing*[248] phenomenon, and more recently the *user-generated video sharing*[249] phenomenon, are finally shedding some light on the inconvenient truth: we have not yet demonstrated a sustainable competitive model for moving raw bits around. Not that we excel at competitive models for moving things around over large distances to almost anywhere. Witness railroads, water, electricity, highways, postal service, telephony. Soon, airlines. The economics clearly need some *sunlight*[250]. And the *p2p*[251] *debate*[252] *will*[253] *require*[254] *some*[255].

240 **The Wealth of Networks: How Social Production Transforms Markets and Freedom, Oct 2007**, http://www.amazon.com/Wealth-Networks-Production-Transforms-Markets/dp/0300125771/
241 **Proceedings of the Twenty-Fourth Internet Engineering Task Force, Jul 1992**, http://www3.ietf.org/proceedings/prior29/IETF24.pdf
242 **Internet growth**, http://www.nic.funet.fi/index/FUNET/history/internet/en/kasvu.html#nimet
243 **"A Look At The Unidentified Half of Netflow", Jan 2008**, http://www.uoregon.edu/~joe/missing-half/missing-half.pdf
244 **Histories of the Internet**, http://www.isoc.org/internet/history/
245 **The Future of the Internet: Q&A with K. Claffy**, http://blog.caida.org/best_available_data/2007/07/
246 *See footnote 117*
247 **"Property, Commons, and the First Amendment: Towards a Core Common Infrastructure", Mar 2001**, http://www.benkler.org/WhitePaper.pdf
248 http://en.wikipedia.org/wiki/P2P_file_sharing
249 http://en.wikipedia.org/wiki/List_of_video_sharing_websites
250 **"The Internet as emerging critical infrastructure: what needs to be measured?", Sep 2007**, http://www.caida.org/publications/presentations/2007/critimeas2007-09/
251 **"Cisco: P2P Flat in North America? Some Experiencing Major Growth", Jul 2008**, http://www.circleid.com/posts/86201_cisco_p2p_flat_in_north_america/
252 **"Sandvine: close to half of all bandwidth sucked up by P2P", Jun 2008**, http://arstechnica.com/news.ars/post/20080623-sandvine-close-to-half-of-all-bandwidth-sucked-up-by-p2p.html
253 *See footnote 233*
254 **"The Effect of File Sharing on Record Sales: An Empirical Analysis", Dec 2006**, http://www.unc.edu/~cigar/papers/JPE%2031618%20FileSharing%202006-12-12.pdf
255 **"Challenges and Directions for Monitoring P2P File Sharing Networks or Why My Printer Received a DMCA Takedown Notice", Aug 2001**, http://dmca.cs.washington.edu/uwcse_dmca_tr.pdf

C. As with most infrastructure issues, the U.S. federal government is *slow to respond*[256] regarding a *national broadband strategy*[257]. But the USG is investing resources and regulatory attention in the to help foster global Internet growth, including: encouraging *IPv6 deployment*[258] to mitigate the coming address space crunch; *improving*[259] the *security of the naming system*[260] with *community-developed standards*[261] for *authenticated DNS*[262] responses; and, in partnership with industry and academia, developing a *roadmap*[263] for federal research and development in cybersecurity and information assurance. (Yes, the emphasis is on security and sustainability issues, but that's where federal investment is today.)

D. With infrastructure, progressive movement tends to begin at the state and *local*[264] levels as *governments*[265] *experiment with*[266] *alternative*[267] *ownership models*[268] for provisioning Internet infrastructure via public-private partnerships. Local experimentation is critical, and eye-opening: after a decade of pay-per-minute hotspots, airports are realizing that free (as in beer) *wifi access*[269] appeals to visitors and residents.

E. The OECD now considers the Internet *relevant to its mission*[270], and is issuing balanced recommendations based on its best available data, which they forcefully admit is problematic. In their recent *ministerial meeting*[271] on the future of the Internet, they committed to "improving statistical indicators to measure access and use of the Internet..in order to provide more reliable data and analysis." Only in the U.S. do policy makers *believe that OECD rankings are lying*[272].

F. There are many *educated*[273] people speaking out on the topic of *informing policy based on what we know*[274], and *reserving judgment*[275] else-

256 **"Whatever happened to the Bush broadband policy?"**, http://isen.com/blog/2005/05/whatever-happened-to-bush-broadband.html
257 *See footnote 131*
258 *See foonote 20*
259 **DNSSEC (Domain Name System Security Extensions) Deployment Initiative**, http://en.wikipedia.org/wiki/DNSSEC#DNSSEC_Deployment_Initiative
269 **DNS security**, http://www.cybertelecom.org/dns/security.htm
261 **DNS Security Introduction and Requirements**, http://www.ietf.org/rfc/rfc4033.txt
262 http://en.wikipedia.org/wiki/DNSSEC
263 **Cyber Security and Information Assurance (CSIA)**, http://www.nitrd.gov/pubs/2008supplement/08-Supp-Web/TOC%20Pages/08supp-CSIA.pdf
264 **"ConnectKentucky's incumbent-centric model cannot meet US broadband needs"**, http://www.muniwireless.com/
265 **Telecommunications network for Burlington**, http://www.burlingtontelecom.com/
266 **"Philadelphia revives citywide Wi-Fi project" , Jun 2008**, http://www.reuters.com/article/technologyNews/idUSN1737601520080617
267 **More about the report and analysis of the Philadelphia Wireless project**, http://www.saschameinrath.com/2008/mar/12/more_thoughts_philly_three_months_after_philadelphia_story
268 **"City Takes Back Wi-Fi Net It Sold to EarthLink", Apr 2008**, http://www.nytimes.com/idg/IDG_852573C4006938800025742E006429B9.html?ref=t
269 **Guide to WiFi in airports world-wide**, http://www.jaunted.com/maps/Airport-WiFi-Map
270 **OECD proposes roadmap for the future of the Internet economy, Jun 2008**, http://www.oecd.org/document/18/0,3343,en_2649_37441_40862162_1_1_1_1,00.html
271 **OECD Ministerial Meeting on the Future of Internet Economy, Jun 2008**, http://www.oecd.org/site/0,3407,en_21571361_38415463_1_1_1_1_1,00.html
272 **"The UK Broadband Infrastructure And the Debate We Should Be Having", Jun 2008**, http://www.wetmachine.com/item/1228
273 **"The Key Questions About the New FISA Bill", Jun 2008**, http://balkin.blogspot.com/2008/06/key-questions-about-new-fisa-bill.html
274 **"Follow Up On Medical Devices: Smarter Devices And Smarter Policy, Not More Bandwidth", Apr 2008**, http://www.wetmachine.com/item/1172
275 **"Reserving Judgment on Sprint/Clearwire/Google/Intel/ForcesofDarkness Deal", May 2008**, http://www.wetmachine.com//item/1180

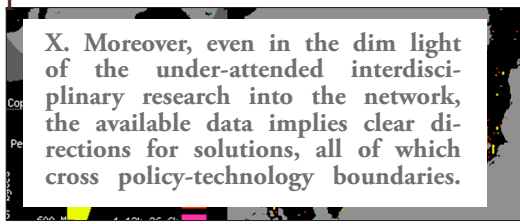
where. (*Recommended thinkers*[276].) There are *evolutionary lessons and insights*[277] to glean from other networked fields facing similar problems, e.g., *semantic web in big pharma*[278] and *efficient routing*[279] as well as lessons to draw from ideas we have tried that have not worked yet, such as *public catalogs*[280] or *open commerce in network data*[281]. There's plenty of work to do, but there's no shortage of qualified people.

G. Authors and journalists have *captured*[282] and *interpreted history*[283], and academic researchers have done their share of *capturing*[284] and *interpreting*[285] the *history of communications*[286] and its implications for the Internet. There is detailed understanding of the history of many aspects of the Internet, including how pieces of the *co-evolving complex systems*[287] of technology, economics, and regulation fit together.

H. Relatively few government-funded researchers, *led by*[288] U.S. federal agency ARPA, supported by *strong regulatory protection for innovation*[289]built the Internet in an amazingly short time relative to the history of communications. Within twenty years the new ecosystem *fatally threatened*[290] the old. The obvious response by the incumbent carriers was to manipulate the regulatory architecture away from the line-sharing that made innovations such as the Internet possible. No surprise there, these same *carriers*[291] *fought*[292] *innovation*[293] *last*[294] *century*[295] too, including *the Internet*[296]. Regulating protection of innovation at the edge is neither new nor somehow obviated by the technological developments of the Internet. On the contrary, the technological ability to innovate at the edge of the Internet is easy to remove in the middle by a network owner. So as with the rest of history of telecom, and as with other social goals such as universal access, it will largely be a matter of pointing legislatures to *results achieved*[297] from *other policies*[298].

"But, important as these problems are, they were not the main point. The main point of the book is to see these human constructions as systems, not as collections of individuals or representatives of ideologies. From our opening accident with the coffeepot and job interview through the exotics of space, weapons, and microbiology, the theme has been that it is the way the parts fit together, interact, that is important. The dangerous accidents liein the system, not in the components. The nature of the transformation process eludes the capacities of any human system we can tolerate in the case of nuclear power and weapons; the air transport system works well — diverse interests and technological changes support one another; we may worry much about the DNA system with its unregulated reward structure, less about chemical plants; and though the processes are less difficult and dangerous in mining and marine transport, we find the system of each is an unfortunate concatenation of diverse interests at cross-purposes. These systems are human constructions, whether designed by engineers and corporate presidents, or the result of unplanned, unwitting, crescive, slowly evolving human attempts to cope. Either way they are very resistant to change. Private privileges and profits make the planned constructions resistant to change; layers upon layers of accommodations and bargains that go by the name of tradition make the unplanned ones unyielding. But they are human constructions, and humans can destruct them or reconstruct them. The catastrophes send us warning signals. This book has attempted to decode these signals: abandon this, it is beyond your capabilities; redesign this, regardless of short-run costs; regulate this, regardless of the imperfections of regulation. But like the operators of TMI (three-mile island) who could not conceive of the worst — and thus could not see the disasters facing them — we have misread these signals too often, reinterpreting them to fit our preconceptions. Better training alone will not solve the problem, or promise that it won't happen again. Worse yet, we may accept the preconception that military superiority and private profits are worth the risks. This book's decoding asserts that the problems are not with individual motives, individual errors, or even political ideologies. The signals come from systems, technological, and economic. They are systems that elites have constructed, and thus can be changed or abandoned."
–Normal Accidents, Charles Perrow, 1999

point ten

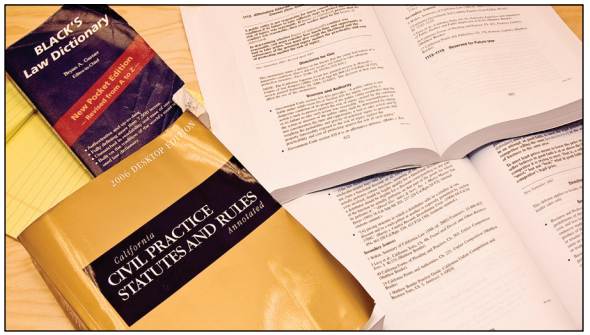


A. We can learn from our mistakes. The false assumption that competing members of a profit-maximizing ecosystem will cooperate toward architectural innovations not in their short-term interest is remarkably consistent across failed attempts to *solve*[299] major *problems of the Internet*[300] (e.g., *ATM*[301], *multicast*[302], *routing secu-*

276 http://blog.caida.org/best_available_data/recommended-feeds/
277 **Evolution of Networks: From Biological Nets to the Internet and WWW, Mar 2003**, http://www.amazon.com/Evolution-Networks-Biological-Internet-Physics/dp/0198515901/
278 **"Pharma Researchers Adopt An Orphan Internet Standard", Oct 2007**, http://pubs.acs.org/email/cen/html/100807150541.html
279 **"Navigability of Complex Networks", Sep 2007**, http://arxiv.org/abs/0709.0303
280 *See footnote 190*
281 *See footnote 194*
282 **Where Wizards Stay Up Late: The Origins Of The Internet, Jan 1998**, http://www.amazon.com/Where-Wizards-Stay-Up-Late/dp/0684832674/
283 **What the Dormouse Said: How the Sixties Counterculture Shaped the Personal Computer Industry, Feb 2006**, http://www.amazon.com/What-Dormouse-Said-Counterculture-Personal/dp/0143036769/
284 **Internet history archive**, http://internethistoryarchive.org/
285 **"Licensing in the Web 2.0 Era", Jul 2007**, http://itc.conversationsnetwork.org/shows/detail3365.html
286 **"The history of communications and its implications for the Internet", Jun 2000**, http://www.dtc.umn.edu/~odlyzko/doc/history.communications0.pdf
287 **"The Telecommunications Economy and Regulation As Coevolving Complex Adaptive Systems: Implications for Federalism"**, http://quello.msu.edu/complexity/CherryTPRC04.pdf
288 **J.C.R. Licklider**, http://en.wikipedia.org/wiki/Licklider
289 Computer Inquiries, http://www.cybertelecom.org/ci/
290 **"Economist: How The Internet Killed the Phone Business", Sep 2005**, http://techliberation.com/2005/09/28/economist-how-the-internet-killed-the-phone-business/
291 **History of AT&T**, http://www.cybertelecom.org/notes/att.htm
292 **Customer Premises Equipment Part 68**, http://www.cybertelecom.org/ci/cpe.htm
293 **Hush-a-phone case**, http://www.cybertelecom.org/library/hushaphone.htm
294 **Carterfone case**, http://www.cybertelecom.org/library/carterfone.htm
295 **AT&T AntiTrust Suit III: Bell Operating Companies,** http://www.cybertelecom.org/notes/att_antitrust.htm#div
296 *See footnote 289*
297 **OECD Broadband Portal**, http://www.oecd.org/document/54/0,3343,en_2649_34225_38690102_1_1_1_1,00.html
298 **"Explaining International Broadband Leadership", May 2008**, http://www.itif.org/index.php?id=142
299 **IAB Concerns and Recommendations Regarding Internet Research and Evolution, Aug 2004**, http://www.ietf.org/rfc/rfc3869.txt
300 *See footnote 62*
301 http://en.wikipedia.org/wiki/Asynchronous_Transfer_Mode#Successes_and_failures_of_ATM_technology
302 http://en.wikipedia.org/wiki/IP_Multicast#History_and_milestones

rity[303], *IPv6*[304], *DNSSEC*[305], *QOS*[306]). Engineers have made valiant efforts to provide architectural solutions to security and scalability problems, providing vivid illustrations of how the *computational thinking*[307] approach, embracing modularization and separation of issues, can fail to account for how tightly linked the technology, economic, and social dimensions of the problems are. As the Internet becomes the substrate underlying our professional, personal and political lives, we must recognize the links within and across its four biggest problems:
(1) the fundamentally *insecure*[308] *software*[309] *ecosystem*[310], (2) *the*[311] *fundamentally*[312] *unscalable*[313] *routing*[314] and *addressing architecture*[315], (3) the *fundamentally*[316] *unsustainable*[317] *economic*[318] *architecture*[319], and (4) a *stewardship*[320] model *broken*[321] along so many *dimensions*[322] that *solving*[323], or even *studying*[324], the first three *problems*[325] is no one's responsibility. Expecting he private sector to navigate these dimensions (security, scalability, sustainability, and stewardship) while subject to relentless pressure to minimize costs is a recipe for failure; even public-private partnerships are not *free of*[326] these *pressures*[327]. Furthermore, since all four dimensions transcend the jurisdiction of any sovereign government, we also cannot expect any solution that emphasizes national boundaries.

B. While competing in the middle prohibits architectural innovation, cooperating at the edge seems to be a common ingredient of the most successful innovations on the Internet, including the web and search engines, VOIP, Linux, Wikipedia, Ebay, the blogosphere and other social networks. Ubiquitous connectivity is transforming economic conditions, supporting collaborations among individuals that achieve *more efficient*[328] means of production and consumption than either government programs or competitive markets have achieved. This transformation leaves some incongruity about *current*



economic architecture[329] for the Internet, which has a deeply embedded *preference for markets*[330] and *private sector control*[331] of *communications infrastructure*[332] as well as *information*[333]. The extremely dynamic and unpredictable structure, usage, and growth of the Internet does not reduce the *necessity of regulation*[334] to well-functioning markets; on the contrary, its elusive nature is what makes *transparent*[335] and *accountable*[336] *experimentation*[337] so necessary.

C. What we believe about the infrastructure influences our technology and policy decisions. The current barriers to data access leave us without any mechanism to verify claims or weed out false beliefs about the infrastructure, including the increasing suspicion that the majority of Internet traffic represents illegal activity. Copyright infringement, only one example, may be so rampant as to be economically unviable to pre vent, but without an *objective*[338] look at how the network is used, we are subject to vain attempts to *criminalize typical network*[339] usage rather than updating the laws to accomplish *their intended purpose*[340] in light of technological developments. Ironically, traffic measurement undertaken by law enforcement for *national seurity purposes*[341] and *attempted*[342] by scientific *researchers*[343] is also *arguably illegal*[344] under current anachronistic legislation. Again, our choice is to cripple socially important goals — law enforcement and *scientific Internet research*[345] — or *update*[346] the

303 **A Survey of BGP Security Issues and Solutions**, http://www.cs.purdue.edu/homes/ninghui/readings/TruSe_fall04/td-5ugj33.pdf
304 **Technical and Economic Assessment of Internet Protocol Version 6 (IPv6)**, http://www.ntia.doc.gov/ntiahome/ntiageneral/ipv6/draft/draftchap4.htm
305 *See footnote 31*
306 **Considerations of Provider-to-Provider Agreements for Internet-Scale Quality of Service (QOS), Mar 2008**, http://www.ietf.org/rfc/rfc5160.txt
307 **Computational Thinking, Mar 2004**, http://www.cs.cmu.edu/afs/cs/usr/wing/www/publications/Wing06.pdf
308 **Online Identity Theft, Jun 2008**, http://www.oecd.org/document/59/0,3343,en_2649_34223_40830139_1_1_1_1,00.html?rssChId=34223
309 **Economics Malware: Security Decisions, Incentives and Externalities, May 2008**, http://www.oecd.org/dataoecd/53/17/40722462.pdf
310 **Daily Submission Volume, Aug 2008**, http://isc.sans.org/submissions.html
311 http://www.wireless-safety.org/
312 **"Scalability of Routing: Compactness and Dynamics"**, http://www.ietf.org/proceedings/06nov/slides/RRG-3.pdf
313 *See footnote 89*
314 **"Damping BGP", Jun 2007**, http://www.potaroo.net/ispcol/2007-06/dampbgp.html
315 **"Report from the IAB Workshop on Routing and Addressing", Sep 2007**, http://www.ietf.org/rfc/rfc4984.txt
316 **"Broadband pricing: solutions that are orthogonal to any real problem", Jun 2008**, http://www.networkworld.com/columnists/2008/061708-bradner.html?fsrc=rss-bradner
317 *See footnote 181*
318 **"The (un)Economic Internet"**, http://www.caida.org/publications/papers/2007/ieeecon/
319 **"$200 Billion Broadband Scandal"**, http://www.newnetworks.com/broadbandscandals.htm
320 See footnote 39
321 **ICANN - The Case for Reform, Feb 2002**, http://www.icann.org/en/general/lynn-reform-proposal-24-feb02.htm
322 **The Broadband Problem: Anatomy of a Market Failure and a Policy Dilemma, Jun 2004**, http://www.amazon.com/Broadband-Problem-Anatomy-Failure-Dilemma/dp/0815706448/
323 *See footnote 160*
324 *See footnote 62*
325 **IPv4 Census Map**, http://www.caida.org/research/id-consumption/census-map/
326 **"Connected Nation's Private Interests Hit In FCC Comments", Jul 2008**, http://www.publicknowledge.org/node/1675
327 http://www.muniwireless.com/2008/01/17/the-connectkentucky-model-a-limited-step-in-the-right-direction/

328 **"Sharing Nicely", 2004**, http://benkler.org/SharingNicely.html
329 http://blog.caida.org/best_available_data/2007/10/07/internet-infrastructure-economics-top-ten-things-i-have-learned-so-far/
330 **"Let There Be Markets: The Evangelical Roots of Economics", May 2005**, http://www.mindfully.org/Industry/2005/Evangelical-Economics1may05.htm
331 **Administration NII Accomplishments**, http://www.ibiblio.org/nii/NII-Accomplishments.html
332 **"The 700 MHz Auction as the Next Front In the Cable/Telco War", May 2007**, http://www.wetmachine.com/totsf/item/789
333 **Intellectual Property and the National Information Infrastructure**, http://www.uspto.gov/web/offices/com/doc/ipnii/
334 **Understanding Regulation: Theory, Strategy, and Practice, Jul 1999**, http://www.amazon.com/Understanding-Regulation-Theory-Strategy-Practice/dp/0198774389/
335 **Sunlight Foundation**, http://www.sunlightfoundation.com/
336 **"Harnessing Conflict and Competitiveness for Society's Benefit", Aug 2000**, http://www.davidbrin.com/disputationarticle1.html
337 **GNU General Public License, Jun 2007**, http://www.fsf.org/licensing/licenses/gpl.html
338 *See footnote 210*
339 http://www.eff.org/riaa-v-people
340 *See footnote 229*
341 **U.S. Code Collection: Chapter 36-Foreign Intelligence Surveillance, Aug 2008,** http://www.law.cornell.edu/uscode/html/uscode50/usc_sup_01_50_10_36.html
342 http://blog.caida.org/best_available_data/2007/08/26/what-we-cant-measure-on-the-internet-reprisal/
343, 344 *See footnote 199*
345 **"Why We Don't Know How To Simulate The Internet", Dec 1997**, ftp://ftp.ee.lbl.gov/papers/wsc97.ps
346 *See footnote 8*

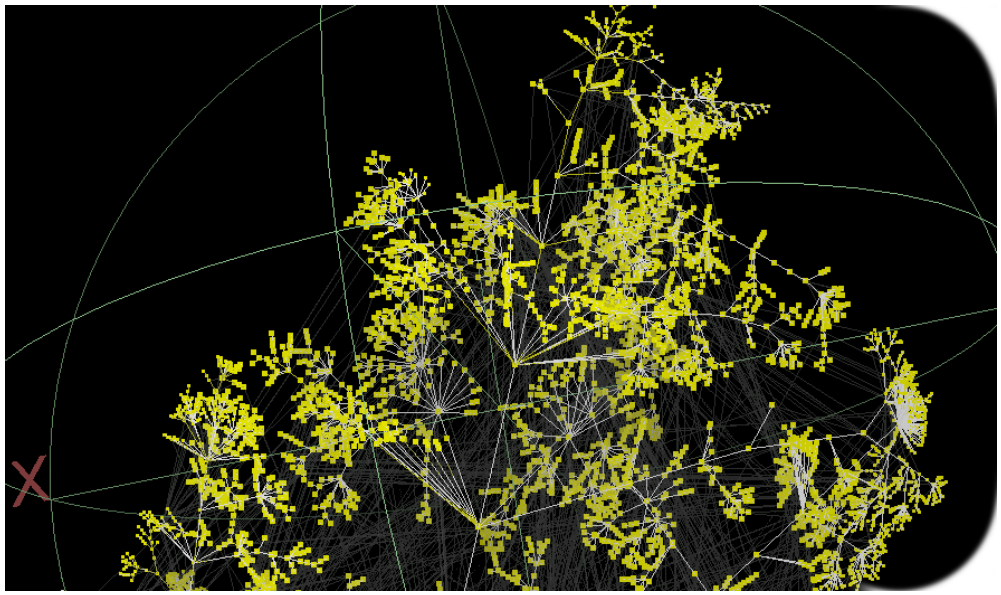
relevant[347] *communications*[348] *privacy*[349] (*ECPA*[350]) legislation.

D. Public investment in knowledge production, including science and medical research, gains enormously from universal connectivity, offering distribution of resulting products to all taxpayers at zero marginal cost. The same reasoning reduces the justification for strong intellectual property systems, since they require expensive technology to prevent networks from doing what networks do naturally: share data. It is thus in interest of taxpayers for governments to promote and sometimes *directly fund*[351] universal deployment of network infrastructure. More generally, government needs to prevent monopoly control over *essential resources*[352], mandate collection of *traffic reports from ISPs*[353] to validate their claims, be a better role model for operational security, and coordinate the development of a road map for Internet security similar to that of the *energy sector*[354] (DHS is working on this last one).

E. Scientific researchers are in a difficult position, trying to do *science without data*[355], but they are in a position to make progress, with the help of a few good legal experts. They (we) could propose a list of the most important Internet research questions/problems to investigate, such as the ongoing *discrepancies*[356] between *supposedly scientific studies*[357], and suggest what data is needed to investigate them. The academic community could even use *existing assets*[358] such as *their own under-utilized backbone*[359] to mitigate the data dearth, by incenting measurement data out of cooperating networks in exchange for network bandwidth. In the process they could help local communities experiment with and measure performance, cost, and efficiency of alternative network ownership models. Internet2 should also work with researchers and their *institutional review boards*[360] (IRBs) at member universities to assist researchers in developing *privacy-respecting*[361] network analysis technologies and data handling policies, so that the organization can share more data from its research backbone with scientific researchers.

F. The FCC is not exempt from the facts either — the agency should be pursuing *empirically grounded validation*[362] of the claimed efficiency of its own policies, even if it requires trading *temporary spectrum unlicensing*[364] as an experiment to gather realistic baseline data on wireless network behavior to policy makers. The academic community could even help design such a network, geared toward public safety objectives and supporting scientific research balanced carefully against individual privacy. Such a trade seems less extreme an idea in light of the failure of the D-block auction, and the FCC admission that economic conditions make it a *bad time to try to auction it now*[365]. Reforming our policy for this spectrum could achieve *efficiency*[366], *access*[367], public safety, and network science objectives at least cost to taxpayers.

"We can have facts without thinking but we cannot have thinking without facts." — John Dewey



347 **U.S. Code Collection: 2511. Interception and disclosure of wire, oral, or electronic communications prohibited, Aug 2008**, http://www.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00002511----000-.html

348 **U.S. Code Collection: Unlawful access to stored communications**, **Aug 2008**, http://www.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00002701----000-.html

349 **"Privacy Act II", Jul 2008**, http://www.fcw.com/online/news/153289-1.html

350 **Electronic Communications Privacy Act**, http://en.wikipedia.org/wiki/ECPA

351 **Broadband Opportunities for Rural America**, http://wireless.fcc.gov/outreach/index.htm?job=broadband_home

352 **The Essential Facilities Doctrine In The Deregulated Telecommunications Industry, 1998**, http://www.law.berkeley.edu/journals/btlj/articles/vol13/Soma/html/reader.html

353 **Internet 3.0: Identifying Problems and Solutions to the Network Neutrality Debate, Jun 2007**, http://ijoc.org/ojs/index.php/ijoc/article/download/160/86

354 **Roadmap to Secure Control Systems in the Energy Sector, January 2006**, http://www.controlsystemsroadmap.net/

355 *See footnote 342*

356 **Internet2 and Quality of Service: Research, Experience, and Conclusions, May 2006**, https://www.educause.edu/ir/library/pdf/CSD4577.pdf

357 *See point five*

358 **High-speed academic networks and the future of the Internet, May 2008**, http://arstechnica.com/articles/culture/future-internet.ars

359 http://www.internet2.edu/

360 **"IRBs and Security Research: Myths, Facts and Mission Creep", Mar 2008**, http://www.usenix.org/events/upsec08/tech/full_papers/garfinkel/garfinkel_html/

361 **1st ACM Workshop on Network Data Anonymization, 2008**, http://www.ics.forth.gr/~antonat/nda08.html

362 **1st ACM Workshop on Network Data Anonymization, 2008**, http://www.ics.forth.gr/~antonat/nda08.html

363 **How To Give America Wireless Broadband For Christmas 2009 - the Lesson from 3.65 GHz Deployment, Jan 2008**, http://www.wetmachine.com/item/1029

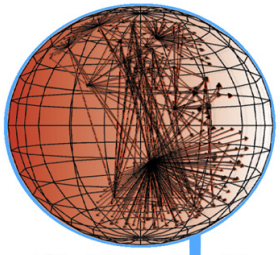
364 **"FCC chief says economy could hurt wireless sale", Jan 2008**, http://www.reuters.com/article/technologyNews/idUSN1555479420080115

365 **"Gaping Hole in Models for Using Spectrum Efficiently", Mar 2008**, http://www.circleid.com/posts/832812_models_wireless_spectrum/

366 **Report: US must have universal gigabit broadband by 2015, Jun 2008**, http://arstechnica.com/news.ars/post/20080624-report-us-must-have-universal-gigabit-broadband-by-2015.html

MADE POSSIBLE BY OUR SPONSORS

AUTHOR: KIMBERLY CLAFFY, **DESIGN**: CONNIE LYU



caida
www.caida.org

University of California
San Diego

Cisco Systems

SDSC
SAN DIEGO SUPERCOMPUTER CENTER

This pamphlet was produced as part of the COMMONS, a CAIDA and Cisco collaborative project, to simultaneously solve three acute and growing problems facing the Internet: a self-reported financial crisis in the Internet infrastructure provider industry; a data acquisition crisis which has severely stunted the field of network science; and a struggle for survival within emerging community and municipal networks.

COOPERATIVE ASSOCIATION FOR INTERNET DATA ANALYSIS
SAN DIEGO SUPERCOMPUTER CENTER. UNIVERSITY OF SAN DIEGO
500 GILMAN DRIVE, MC0505. LA JOLLA, CA 92093-0505.
858-534-5000. http://www.caida.org/