FOXES AND HEDGEHOGS IN TRANSITION

DEREK E. BAMBAUER*

INTRODUCTION

The migration from a congeries of communications protocols and technologies to an Internet Protocol-based system is an architectural shift of profound magnitude: it is as though people returned to the city of Babel, abandoning their native tongues for a single lingua franca. Perhaps, after this shift, nothing will be restrained from those who use the Internet.[1] And yet, there will inevitably be problems that arise from the shift. Scholars and activists have already raised concerns about equal access to communications capabilities; about the security and resiliency of the new architecture; and about the tension between competing speech interests on the network.

One way of thinking about these problems, and potential solutions, is to classify them as either hedgehogs or foxes. The British philosopher Isaiah Berlin suggested that intellectuals can be classified into these two camps, puckishly borrowing from the Greek poet Archilochus, who observed that "the fox knows many things, but the hedgehog knows one big thing."[2] A hedgehog problem is predictable: it flows directly from the

* Professor of Law, University of Arizona James E. Rogers College of Law. Thanks for helpful suggestions and discussion are owed to Jane Bambauer, Dan Hunter, Thinh Nguyen, and the participants at the Digital Broadband Migration: After the Internet Protocol Revolution conference at the University of Colorado. The author welcomes comments at <derekbambauer@email.arizona.edu>.

1. *See Genesis* 11:6 ("And the Lord said, Behold, the people is one, and they have all one language; and this they begin to do: and now nothing will be restrained from them, which they have imagined to do.").

2. ISAIAH BERLIN, THE HEDGEHOG AND THE FOX 1 (Henry Hardy ed., Princeton Univ. Press, 2nd ed. 2013) (1953).

transition, and is largely invariant across contexts. A solution to a hedgehog problem should work in most if not all cases. A fox problem is contextual: its effects are indirect, and depend on the circumstances. Fixes must necessarily be more tailored, and are harder to envision in advance. The classification exercise is useful regardless of its outcome. Hedgehog problems offer generalizable answers—solutions that are broadly applicable and hence well worth the effort to obtain. Fox problems do not provide this advantage; they are bespoke challenges with largely unique solutions. However, fox problems helpfully challenge regulators, and society more broadly, to elucidate and consider the principles used to arrive at individualized responses. Grouping transition issues into two camps can help us economize on remediation and evaluate underlying normative commitments.

The unifying move onto Internet Protocol (IP) will unsettle—for good and ill—a host of social practices, legal doctrines, and technologies. This essay considers three of these disruptions: the decreased resiliency of a monolithic protocol architecture (a hedgehog problem), the destabilization of universal service arrangements (a fox problem), and the unmooring of constitutional protections from speech from their historical and technological roots (also a fox problem). All three require us to revisit choices, and value judgments, long thought settled. The essay closes with some normative suggestions for how those debates ought to proceed.

I. A FLATTER NETWORK

The transition to IP inevitably reduces the diversity of communications protocols, at least at the routing layer. Different media, in our current conception, become simply different applications.[3] Broadcast television, Hulu, and YouTube converge.[4] Text messaging and GChat and Twitter compete. We will increasingly define modes of

3. Douglas C. Sicker, *The End of Federalism in Telecommunication Regulation?*, 3 NW. J. TECH. & INTELL. PROP. 130, 153-54 (2005).

4. Walter S. Ciciora, *Cable Television in the United States: An Overview*, CABLELABS, 4-10 (rev. 2nd ed. May 25, 1995), *available at* http://people.seas.harvard.edu/~jones/cscie129/nu_lectures/lecture13/pdf/CATV.pdf; *see* Susan P. Crawford, *The Radio and the Internet*, 23 BERKELEY TECH. L.J. 933, 961-62 (2008) (stating that both broadcast and cable television routing become more complex with IP; broadcast simply involved transmission of signal in an assigned part of the electromagnetic spectrum); Lynn Claudy, *TV's Future: The Broadcast Empire Strikes Back*, IEEE SPECTRUM (Nov. 29, 2012), http://spectrum.ieee.org/consumer-electronics/audiovideo/tvs-future-the-broadcast-empire-strikes-back; *see generally* U.S. DEP'T OF COMMERCE, UNITED STATES FREQUENCY ALLOCATIONS: THE RADIO SPECTRUM (2003), http://www.ntia.doc.gov/files/ntia/publications/2003-allochrt.pdf (showing cable depended upon a dedicated physical network between provider and consumer).

communication via functionality rather than by how they are transmitted, or by the device one uses to employ them. This is plainly a feature and not a bug: consolidation is an express goal of the transition. Yet, it is not without difficulties.

One challenge is that resiliency declines when all traffic routes using IP. Any problem that affects IP routing—including deliberate attacks—will affect an increasing number of communications media. The routing level is increasingly a monoculture, creating potential efficiencies and also significant vulnerabilities.[5] An infrastructure with diverse protocols is harder to manage, and also harder to attack.[6] This is a hedgehog problem: decreased resiliency affects users and applications in the same way, and is likely amenable to the same fix. Pre-transition, an attack or bug affecting IP routing might knock out Internet communications, but would leave standard telephone service untouched, because the phone system principally employs a different protocol: Time-Division Multiplexing (TDM).[7] Post-transition, when phone calls operate via voice over IP, a problem with IP will disrupt them as well. Large-scale disruptions to connectivity increasingly wreak havoc, from natural disasters (such as Hurricane Sandy) to human-generated accidents (such as the severing of undersea cables) to deliberate attacks (such as the denial-of-service attacks against Estonia and Georgia).[8] And while physical carriage remains diverse—cable modems, DSL, wireless, and even pigeons can carry traffic[9]—the larger IP ecosystem has coalesced onto a few key points of vulnerability, such as Border Gateway Protocol (BGP)[10], associated memory limits in some routing equipment[11], and limits to IPv4 addresses[12] Any interruption that affects

5. Derek E. Bambauer, *Ghost in the Network*, 162 U. PA. L. REV. 1011, 1058-62 (2014).

6. *Id.* at 1061.

7. *See generally* Tim Greene, *VoIP vs. TDM voice*, NETWORKWORLD (Oct. 26, 2007, 1:00 AM), http://www.networkworld.com/news/2007/102607-arguments-voip-tdm.html.

8. *See* Derek E. Bambauer, *Conundrum*, 96 MINN. L. REV. 584, 653-58 (2011).

9. Memorandum from D. Waitzman on RFC 1149: A Standard for the Transmission of IP Datagrams on Avian Carriers (Apr. 1, 1990), *available at* http://www.rfc-editor.org/rfc/rfc1149.txt.

10. Memorandum from Y. Rekhter, T. Li, & S. Hares on RFC 4271: A Border Gateway Protocol (BGP-4) (Jan. 2006), *available at* http://www.rfc-editor.org/rfc/rfc4271.txt.

11. Drew Fitzgerald, *Echoes of Y2K: Engineers Buzz That Internet Is Outgrowing Its Gear*, WALL ST. J. (Aug. 13, 2014, 7:48 PM), http://online.wsj.com/articles/y2k-meets-512k-as-internet-limit-approaches-1407937617; Robert Lemos, *Internet Routers Hitting 512K Limit, Some Become Unreliable*, ARS TECHNICA (Aug. 13, 2014, 1:03 PM), http://arstechnica.com/security/2014/08/internet-routers-hitting-512k-limit-some-become-unreliable/.

12. Scott Hogg, *ARIN Enters Phase 4 of IPv4 Exhaustion*, NETWORKWORLD (Apr. 23, 2014, 10:35 AM), http://www.networkworld.com/article/2226785/cisco-subnet/arin-enters-phase-4-of-ipv4-exhaustion.html.

IP routing threatens to block an increasing number of modes of communication, from voice, to e-mail, to SMS.

Disruptions to IP routing are not chimerical possibilities. For example, in 2008, Pakistan's Telecommunication Authority directed the country's ISPs to block access to the controversial film "Fitna," which was available on YouTube. Pakistan Telecom went one step further and attempted to block customers' access to YouTube itself.[13] The ISP did so by advertising a BGP route for part of YouTube's network (IP address range).[14] Pakistan Telecom customers who tried to access YouTube would be redirected to a page hosted by the ISP. However, Pakistan Telecom botched the effort: the company advertised the route to its upstream provider, which accepted it.[15] The inaccurate routing information then spread; network firm Renesys estimates that about half of the Internet was exposed to the bad data.[16] For a period of time, Pakistan Telecom received a sizable share of YouTube's requests.[17] ISPs coordinated to restore proper BGP routes quickly, making quality video programming again available to all, but the problem recurs.[18]

Pakistan is not an outlier. In April 2010, China Telecom issued BGP routes for over 50,000 IP addresses that it did not own, diverting traffic for roughly 20 minutes.[19] In December 2013, attackers used BGP weaknesses to reroute traffic—including some from financial institutions and government entities—to locations in Belarus and Iceland.[20] Renesys observed BGP-based man-in-the-middle attacks on over 60 days in 2013, affecting traffic in 150 cities worldwide.[21] BGP's weaknesses are well known; it is a component of IP routing that essentially relies on trust.[22]

13. Martin Brown, *Pakistan Hijacks YouTube*, DYN RESEARCH (Feb. 24, 2008), http://www.renesys.com/2008/02/pakistan-hijacks-youtube-1/.

14. *Id.* (explaining that Pakistan Telecom advertised a more specific route via BGP; for the technically inclined, YouTube advertised 208.65.152.0/22, while Pakistan Telecom advertised 208.65.153.0/24); *see generally* ILJITSCH VAN BEIJNUM, BGP 117-20 (2002).

15. Brown, *supra* note 13.

16. *Id.*

17. *Id.*

18. *See* cotter548, *RickRoll'D*, YOUTUBE (May 15, 2007), http://www.youtube.com/watch?v=oHg5SJYRHA0.

19. Jim Cowie, *China's 18-Minute Mystery*, RENESYS (Nov. 18, 2010), http://www.renesys.com/2010/11/chinas-18-minute-mystery/.

20. Kim Zetter, *Someone's Been Siphoning Data Through a Huge Security Hole in the Internet*, WIRED (Dec. 5, 2013), http://www.wired.com/threatlevel/2013/12/bgp-hijacking-belarus-iceland/; Jim Cowie, *The New Threat: Targeted Internet Traffic Misdirection*, RENESYS (Nov. 19, 2013), http://www.renesys.com/2013/11/mitm-internet-hijacking/; Dan Goodin, *Repeated attacks hijack huge chunks of Internet traffic, researchers warn*, ARS TECHNICA (Nov. 20, 2013), http://arstechnica.com/security/2013/11/repeated-attacks-hijack-huge-chunks-of-internet-traffic-researchers-warn/.

21. Cowie, *supra* note 20.

22. Dan Goodin, *Hacking Internet Backbones – It's Easier Than You Think*, REGISTER (Apr. 16, 2009), http://www.theregister.co.uk/2009/04/16/internet_backbone_hacking/.

The protocol defaults to advertising all of an entity's routes to all other BGP peers.[23] If the advertising computer fails to filter its outbound information, or the peers do not properly limit what routes they accept, inaccurate information spreads easily.[24] The IP transition means that an increased range of communication is subject to inadvertent or deliberate interference with BGP, among other vulnerabilities. And while BGP could be secured, doing so is time-consuming, requires significant coordination, and likely will not occur without a traumatic focusing event that demonstrates the scale of the problem.[25]

Internet policymakers need to think hard about the risk of damage to IP networks. Heterogeneous communications architectures survive disruption better than homogeneous ones. Indeed, outdated technology may even have an advantage in times of crisis. Older networks, such as phone and broadcast radio, let users operate with cheap, tough, low-powered devices. For example, after the 2013 typhoon in the Philippines, the most effective form of communication was one of the simplest: amateur (ham) radio.[26] Ham radio operators are increasingly uncommon. And yet, their basic model can serve as a potential answer to the need for a last-resort means of communication when smartphones fail because cell tower batteries run down, or when PCs falter because cable or phone lines are severed.[27] From Alaska to Egypt, users have resorted to low-tech connectivity when more advanced connections have been severed.[28] Local, user-generated, ad hoc connectivity—in the manner of the New America Foundation's Commotion 1.0[29], or Yochai Benkler's open wireless networks[30]—offers significant potential to remediate network disruptions. However, these capabilities won't emerge on their own. Users or networking firms are unlikely to invest in sufficient redundancy along these lines. Redundancy, after all, is of limited value until disaster strikes, and disasters tend to be unpredictable. This highlights the role of government in driving resiliency: to plan for and invest in disaster

23. BEIJNUM, *supra* note 14, at 135.

24. *Id.*

25. Kim Zetter, *Revealed: The Internet's Biggest Security Hole*, WIRED (Aug. 26, 2008), http://www.wired.com/threatlevel/2008/08/revealed-the-in/; *See* Kevin Butler et al., *A Survey of BGP Issues and Solutions*, 98 PROCEEDINGS OF THE IEEE 100, 105-11 (2010); *see generally* Craig Labovitz, *China Hijacks 15% of Internet Traffic?*, ARBOR NETWORKS (Nov. 19, 2010), http://www.arbornetworks.com/asert/2010/11/china-hijacks-15-of-internet-traffic/.

26. Rachel Martin, *Connecting To The Internet, And The World, Post-Disaster*, NPR (Nov. 17, 2013), http://www.npr.org/templates/story/story.php?storyId=245749083.

27. *Id.*

28. Bambauer, *supra* note 8, at 657.

29. *Commotion Wireless*, OPEN TECH. INST., http://oti.newamerica.net/commotion_wireless_0 (last visited Nov. 12, 2014).

30. Yochai Benkler, *Some Economics of Wireless Communications*, 16 HARV. J.L. & TECH. 25, 46 (2002).

recovery that is not economically rational for other societal actors to undertake.[31]

One possible solution to a less-resilient IP monoculture is to maintain some legacy equipment (and the knowledge of how to use it) in critical sectors, such as emergency services.[32] Redundancy, even with theoretically obsolete technology, acts as a form of insurance.[33] For example, the Hubble Space Telescope uses backup systems that run on Intel 80486 (486) CPUs—state of the art technology, circa 1989.[34] Why? It's reliable.[35] Similarly, the copper wires of the legacy phone system are plainly outdated, but they may well function more reliably than cell phone, cable, or Wi-Fi under conditions of natural disaster or other disruption—consumers' phones (so long as they are not cordless) do not need their own power source, since they can draw from the central office.[36] Communications technologies that do not rely upon IP may be more reliable in certain circumstances, such as if there is a denial-of-service attack or mistake in BGP configuration.[37] IP-based communication is the future, but it remains sensible to retain a foothold in the past. This is a classic hedgehog solution: one big idea (heterogeneity) solves many problems.

Similarly, another useful consideration is to encourage diversity at the physical and link layers.[38] Monoculture at one layer of the protocol

31. *See generally* Philip J. Weiser, Dale Hatfield & Brad Bernthal, *The Future of 9-1-1: New Technologies and the Need for Reform*, 6 J. ON TELECOMM. & HIGH TECH. L. 213, 251-58 (2008) (describing 911 governance); Bambauer, *supra* note 8, at 635-67.

32. The U.S. Navy learned this lesson the hard way. Its Smart Ship program ran most programs aboard the Aegis cruiser USS Yorktown on Windows NT. But when bad data caused a buffer overrun, the ship was dead in the water for two-and-a-half hours and reportedly had to be towed into port. *Sunk by Windows NT*, WIRED (July 24, 1998), http://archive.wired.com/science/discoveries/news/1998/07/13987; Gregory Slabodkin, *Software Glitches Leave Navy Smart Ship Dead In the Water*, GCN (July 13, 1998), http://gcn.com/Articles/1998/07/13/Software-glitches-leave-Navy-Smart-Ship-dead-in-the-water.aspx?Page=1.

33. *See generally* Bambauer, *supra* note 8, at 655-56.

34. J. Mark Lytle, *Ancient 486 PC takes over Hubble telescope*, TECHRADAR (Oct. 17, 2008), http://www.techradar.com/us/news/computing-components/processors/ancient-486-pc-takes-over-hubble-telescope-476221.

35. Andrew Moseman, *Scientists Fixing Hubble Contend With Antiquated Computers*, POPULAR MECHANICS (Oct. 24, 2008, 12:00 AM) (quoting NASA spokesperson Susan Hendrix), http://www.popularmechanics.com/science/space/telescopes/4288705.

36. *See, e.g.*, Gerry Smith, *AT&T, Verizon Phase Out Copper Networks, 'A Lifeline' After Sandy*, HUFFINGTON POST (Nov. 9, 2012, 3:06 PM), http://www.huffingtonpost.com/2012/11/09/att-verizon-sandy_n_2094302.html.

37. Denial of service attacks remain both popular and difficult to defeat. *See, e.g.,* Paul Tassi, *FBI-Hunted Hacking Group Continues Attacks, Targets Twitch*, FORBES (Aug. 27, 2014, 10:15 AM), http://www.forbes.com/sites/insertcoin/2014/08/27/fbi-hunted-hacking-group-continues-attacks-targets-twitch/.

38. *See generally* Bruce Schneier, *Software Monoculture*, SCHNEIER ON SECURITY (Dec. 1, 2010, 5:55 AM), https://www.schneier.com/blog/archives/2010/12/software_monocu.html.

stack is potentially worrisome; monoculture at multiple layers is positively frightening. As I have described elsewhere, this can mean sacrificing efficiency for other goals, such as reliability and resiliency.[39] Perhaps some level of inefficiency is ultimately efficient. Policymakers should assume and plan for disruption. In complex systems, breakdowns are inevitable.[40] Prevention is futile; the only adequate response is to mitigate the damage.[41] Complacency about solutions at the physical layer can lead to unpleasant outcomes. Google assumed the data it synchronized across its private fiber networks was secure, and did not encrypt it—allowing the National Security Agency to access and copy that information.[42] A company that assumed compromise at the physical layer would likely have accelerated encryption of the data.[43] And some New York firms who invested in redundant Internet connections failed to notice that those connections passed through the same Verizon central switching office in lower Manhattan.[44] Those companies found their putatively redundant connections severed when the attacks of September 11, 2001, damaged the switching office.[45]

For all its benefits, the transition to homogeneous IP routing reduces the resiliency of American communications platforms. Fortunately, this one big problem has one broadly applicable fix: retain some diversity in critical sectors such as emergency services, and critical components such as physical connectivity and protocols.

II. UNIVERSAL SERVICE?

The second disruption of the transition to IP will unsettle aspects of the American social contract for communications. The U.S. has accepted that certain technologies ought to be universally available, such as basic voice service and electricity,[46] at low or subsidized rates.[47] We do so for

39. *See* Bambauer, *supra* note 8, at 668–69.

40. Bambauer, *supra* note 5, at 1025-30.

41. *Id.*

42. Barton Gellman & Ashkan Soltani, *NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say*, WASH. POST (Oct. 30, 2013), http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html.

43. Sean Gallagher, *Googlers say "F*** you" to NSA, Company Encrypts Internal Network*, ARS TECHNICA (Nov. 6, 2013), http://arstechnica.com/information-technology/2013/11/googlers-say-f-you-to-nsa-company-encrypts-internal-network/.

44. U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-03-251414, POTENTIAL TERRORIST ATTACKS: ADDITIONAL ACTIONS NEEDED TO BETTER PREPARE CRITICAL FINANCIAL MARKET PARTICIPANTS 92-94 (2003), *available at* http://www.gao.gov/new.items/d03251.pdf.

45. *See* Bambauer, *supra* note 8, at 615-16.

46. *See* U.S. DEP'T OF AGRIC., A BRIEF HISTORY OF THE RURAL ELECTRIC AND

deontological reasons, such as protecting the dignity of all citizens, and for consequential ones, such as making it possible to communicate public safety information. However, the U.S. has not made a broad commitment to universal access to the Internet; America treats broadband (or even dial-up) as a standard market service, where access is mediated by money.[48] These two traditions—universal service for voice, and a market-based approach to Internet—must inevitably clash when the two technologies converge. This is a fox problem: it involves multiple, overlapping, sometimes conflicting normative commitments that must be resolved in contextual fashion. That resolution, though, will highlight which values are compelling enough to drive investment and regulation.

In response to the move to IP, advocacy groups, such as Public Knowledge, have urged the FCC (as a proxy, presumably, for policymakers more generally) to maintain the principles that they claim undergird universal service in the current, copper wire-based phone system: universal service, competition, interconnection, consumer protection, network reliability, and public safety.[49] These are all admirable goals, but there is no particular reason that voice, as an application, need act as their champion.[50] Technology and principles are different. History is not destiny. Telephone communication, as a primary means of social interaction, is an artifact.[51] Increasingly, even e-mail is passé: people and businesses use SMS, social media, and specialized applications such as Snapchat to share information.[52] Similarly, network reliability is a hallmark of the legacy telephone system. The Internet is anything but reliable—indeed, IP routing deliberately discards reliability

TELEPHONE PROGRAMS (1982), *available at* http://www.rurdev.usda.gov/rd/70th/rea-history.pdf; *cf.* FED. COMM'CNS COMM'N, UNIVERSAL SERVICE PROGRAM FOR SCHOOLS AND LIBRARIES (E-RATE) (Apr. 1, 2014), *available at* http://transition.fcc.gov/cgb/consumerfacts/usp_Schools.pdf.

47. *Description of Lifeline Benefits*, UNIVERSAL SERV. ADMIN. CO., http://www.usac.org/li/getting-service/benefits.aspx (last visited Nov. 1, 2014).

48. *See* 47 U.S.C. § 230(b)(1) (1998) (stating that it is a policy goal "to preserve the vibrant and competitive free market that presently exists for the Internet").

49. Jodie Griffin & Harold Feld, *Five Fundamentals for the Phone Network Transition*, PUBLIC KNOWLEDGE (July 24, 2013), http://www.publicknowledge.org/five-fundamentals-phone-network-transition.

50. *See* James E. Holloway & Elaine Seeman, *How Non-Voice Access Technology Is Driving the Creation of Federal and State NG911 Service and IP-Enabled Communications Network Policies*, 31 TEMP. J. SCI. TECH. & ENVTL. L. 59, 78-81 (2012) (describing NG911 system that can receive text and video as well as voice).

51. *See* Amy Gahran, *One-third of Americans prefer texts to voice calls*, CNN (Sept. 22, 2011), http://www.cnn.com/2011/09/22/tech/mobile/americans-prefer-text-messages/.

52. *See, e.g.*, Dara Kerr, *Teens prefer texting over phone calls, e-mail*, CNET (Mar. 19, 2012), http://news.cnet.com/8301-1023_3-57400439-93/teens-prefer-texting-over-phone-calls-e-mail/.

in favor of efficiency.[53] Overall, universal service collapses into one of two goals: either public safety (making this criterion redundant) or cross-subsidization (making it potentially obsolete in favor of a tax and transfer system). Public Knowledge and its fellow travelers have good intentions, but they have simply copied the aspects of the phone system that they like without explaining why the new IP-based network should embody them, rather than using alternative means.

We would do well to move the analysis to a higher level of abstraction: what are the basic, minimal set of communication capabilities we want each American to possess?[54] How should those capabilities be paid for? And what business practices must Internet firms, writ large, engage in, or abstain from, to protect those capabilities and the basic characteristics of the Internet? This set of questions forces us to define the terms of the social contract for communication in the all-IP era. Some aspects are likely uncontroversial: everyone ought to have the capability to call the police or fire department. Some are more difficult: the U.S. has not shown an interest in ensuring universal access to broadband, either via subsidy or via government provision (such as municipal Wi-Fi).[55] And some have changed with time: in the era of analog television, access was near-universal receivers became cheap, but the digital transition left some Americans out.[56] The critical move is to focus not on technologies, but on capabilities, in determining what services ought to be universal in an all-IP world.

Here, I offer a concededly minimalist proposal: the transition should not be regressive. People who utilize, for example, the federal universal service program for low-income consumers should have equivalent service and pricing under the IP model. There are utilitarian considerations that support this position: a community is better off if every citizen can report a fire, crime, or missing child. There are also egalitarian concerns: it is difficult to defend the transition as the Fourth Network Revolution if it makes least-affluent citizens worse off.[57] Revolutions are supposed to empower the downtrodden, not add to their plight. As the costs of creating and distributing information fall, benefits

53. *See* Bambauer, *supra* note 8, at 636.

54. FCC chairman Tom Wheeler has begun to describe these normative commitments as the "Network Compact." Tom Wheeler, *The IP Transition: Starting Now*, OFFICIAL FCC BLOG (Nov. 19, 2013), http://www.fcc.gov/blog/ip-transition-starting-now.

55. In 2011, the Organization for Economic Co-Operation and Development placed the U.S. 14th in households with access to broadband, behind such technology powers as Luxembourg. *Households with Broadband Access*, OECD (last visited Oct. 20, 2014), http://www.oecd.org/sti/broadband/39574039.xls.

56. Eliot Van Buskirk, *How We Bungled the Digital Television Transition*, WIRED (Feb. 20, 2009), http://www.wired.com/business/2009/02/how-the-governm/.

57. Wheeler, *supra* note 54.

should expand, not contract.

A slightly more ambitious proposal would continue the work of President Barack Obama's Broadband Technology Opportunities Program (BTOP), which used economic stimulus funding to subsidize the build-out of broadband connectivity in underserved areas.[58] This encouraged Internet access providers to connect more Americans to broadband, particularly in rural areas.[59] Similarly, the FCC, or government more generally, could examine access in urban areas, both in terms of connectivity and cost. The density of cities makes them good candidates for wireless access, particularly by mobile devices (which reduces the one-off cost for consumers, who can buy a tablet rather than an iPhone). Where urban residents are underserved—and where state laws do not ban governmental provision of broadband—the federal government should consider building out wireless network capacity. Where state laws do prohibit municipal Wi-Fi (inevitably in the service of protecting incumbents), the government should employ a BTOP-like program to encourage Wi-Fi development by Internet access providers, in return for caps on access charges and commitments to non-discrimination and non-blocking regimes.[60]

The IP transition unsettles universal service commitments and values. It pits two conflicting American attitudes against one another: the promise of universal voice service versus a dedication to market-mediated access to broadband IP services. And, it removes an easy technological distinction for divining where the two divide. By examining what set of capabilities we want each citizen to have, with little attention to ability to pay, and by ensuring that no one is worse off from the transition, we can re-define the social compact for communications in the United States.

III. THE CAST OF CHARACTERS

The transition to an all-IP world will press home difficult, lingering questions about freedom to communicate, particularly in constitutional law. First Amendment analysis has long differed by medium, with traditional print and Internet communication receiving the most robust protection against regulation, broadcast media the least, and cable

58. NAT'L TELECOMMS. INFO. ADMIN., *Program Information*, BROADBAND USA, http://www2.ntia.doc.gov/information.

59. *See* CHMN. JULIUS GENACHOWSKI, FED. COMMC'NS COMM'N, BRINGING BROADBAND TO RURAL AMERICA: UPDATE TO REPORT ON A RURAL BROADBAND STRATEGY, GN Docket No. 11-16, 26 FCC Rcd. 8681 (2011)

60. *See generally* Glenn Fleishman *Whatever Happened to Municipal Wi-Fi?*, ECONOMIST (July 26, 2013), http://www.economist.com/blogs/babbage/2013/07/wireless-networks (outlining changes due to municipal broadband since 2004).

television holding an intermediate position.[61] This framework has been the subject of sustained scholarly attack, yet it persists.[62] However, the IP shift will finally either knock away or make absurd the technological underpinnings for this doctrinal divergence. It will also sharpen questions around the rights of listeners or users of communications media, as speaker-centric analysis will increasingly fail to act as a sufficient proxy.[63] This essay next explores the coming crisis in constitutional law, and then turns to the need to develop listener-oriented models of the First Amendment.

Protections for freedom of communication—or, put another way, the burden a government must meet to regulate information—have long varied by medium. Printed media, such as newspapers and magazines, have received the most robust protection.[64] Information transmitted through these channels is generally impervious to content-based regulation, and time/place/manner restrictions are less cogent for print.[65] Internet communication, too, enjoys rigorous safeguards against restrictions.[66] Broadcast television and radio, however, are more amenable to regulation. First Amendment jurisprudence for communications has concentrated on speakers' interests, analyzing whether restrictions on who may speak in a given medium can withstand the presumption against such controls.

To date, however, First Amendment jurisprudence has not fully taken into account listener/reader/user interests in analyzing government regulation of speech.[67] Of the triad of interests—speaker, government, listener—the listener's position gets the least consideration.[68] This occurs

61. *See* Red Lion Broad. Co. v. FCC, 395 U.S. 367 (1969) (radio and television); Miami Herald Publ'g Co. v. Tornillo, 418 U.S. 241 (1974) (newspapers); Fed. Commc'ns Comm'n v. Pacifica Found., 438 U.S. 726 (1978) (radio); Reno v. Am. Civil Liberties Union, 521 U.S. 844 (1997) (Internet); Turner Broad. Sys. v. FCC, 520 U.S. 180 (1997) (cable television).

62. *See, e.g.*, Christopher S. Yoo, *The Rise and Demise of the Technology-Specific Approach to the First Amendment*, 91 GEO. L.J. 245 (2003).

63. *See* Derek E. Bambauer, *Orwell's Armchair*, 79 U. CHI. L. REV. 863, 917-20 (2012) (outlining listener's rights to access information).

64. *Tornillo*, 418 U.S. 241.

65. *See, e.g.*, Ward v. Rock Against Racism, 491 U.S. 781 (1989); Clark v. Cmty. for Creative Non-Violence, 468 U.S. 288 (1984).

66. *See Reno*, 521 U.S. 844; Ashcroft v. Am. Civil Liberties Union, 535 U.S. 564 (2002).

67. Bambauer, *supra* note 63 at 918.

68. There are, of course, exceptions, though they may serve to prove the rule. *See, e.g.*, Va. State Bd. of Pharmacy v. Va. Citizens Consumer Council, 425 U.S. 748, 763 (1976) (describing consumers' "interest in the free flow of commercial information"); Bates v. State Bar of Ariz., 433 U.S. 350, 364 (1977); Red Lion Broad. Co. v. FCC, 395 U.S. 367, 390 (1969) (stating "[i]t is the right of the viewers and listeners, not the right of the broadcasters, which is paramount.") Strangely, these cases principally concern commercial speech, not "core" First Amendment speech such as political discourse.

for at least two reasons. First, listeners are, at times, superfluous to the analysis: their interests are adequately represented by either the speaker (insofar as they wish to receive information)[69] or the government (if they want to be shielded from it)[70] Second, and perhaps as a result, the doctrine is replete with defenses of the right to speak, but contains only suggestions of the right to receive information.[71]

Network neutrality highlights how the transition makes this problem acute. Though the FCC's anti-blocking and anti-discrimination rules are dead again, at least for the moment, the regime they seek to impose would ensure that willing listeners could receive information from willing speakers, even if the intermediary between them objected to the content.[72] Speakers are on weaker ground in mounting a defense of network neutrality or an attack on service providers who filter conduits: there's no constitutional right (yet) to reach a particular listener, and the precedents that compel intermediaries to carry unwanted information apply to broadcast media, not the Net.[73] Even should Verizon decide to block access to Netflix, the telecommunications carrier is not a government actor—there is no state action to challenge.[74] And, Verizon is not preventing Netflix from speaking. It is simply limiting the video service's audience. Under current doctrine, then, debates over network neutrality do not have a constitutional dimension: there is no state action impeding either speakers or listeners; speakers' interests do not seem sufficiently implicated; and it is not clear that listeners possess a First Amendment interest at all.

Yet, there is an additional claimant for freedom to speak: the network providers themselves. ISPs such as Verizon have advanced (although the D.C. Circuit has thus far refrained from assessing) a First Amendment interest in deciding what content may or may not flow across their wires and cables.[75] Network providers seek to align themselves, for the purposes of constitutional analysis, with cable television providers, newspapers, and bookstores, each of which exercises discretion in selecting the content it chooses to make available to consumers. The ISPs are trying to move away from being seen as

69. *See, e.g.*, Lamont v. Postmaster Gen. of U.S., 381 U.S. 301 (1965).

70. *See, e.g.*, Nat'l Socialist Party of Am. v. Vill. of Skokie, 432 U.S. 43 (1977).

71. *See, e.g.*, Martin v. City of Struthers, Ohio, 319 U.S. 141, 143 (1943); Stanley v. Georgia, 394 U.S. 557, 564 (1969); Bd. of Educ., Island Trees Union Free Sch. Dist. No. 26 v. Pico, 457 U.S. 853 (1982).

72. Verizon v. FCC, 740 F.3d 623 (D.C. Cir. 2014).

73. Turner Broad. Sys., Inc. v. FCC, 520 U.S. 180 (1997).

74. *See generally* CBS, Inc. v. Democratic Nat'l Comm., 412 U.S. 94 (1973).

75. Joint Brief for Verizon and MetroPCS at 42-48, Verizon v. FCC, 740 F.3d 623 (D.C. Cir. 2014) (No. 11-1355), *available at* http://gigaom2.files.wordpress.com/2012/07/verizon-metropcs-net-neutrality-brief-as-filed.pdf.

common carriers, like the telephone network, for First Amendment treatment. This is a slightly counterintuitive step: it would be odd if seventy years of federal telecommunications regulation had been unconstitutional, with no one the wiser. The position of the ISPs seems to be that even though, to date, they have engaged in forbearance by not selecting among the content that flows through their pipes, these actions are a matter of corporate grace. A statute mandating carriage against their will would force them to convey information potentially at odds with their positions, or at least against their will.[76]

This set of positions creates an odd dynamic in the constitutional analysis. Internet service providers, whose previous efforts to select among content were limited principally to blocking spam and malware, and who otherwise opened their networks to material of every sort, now claim to have been speakers all along. Should the government manage to surmount extant statutory hurdles and impose network neutrality, courts will have to assess the merits of the ISPs' position. Yet, the government seeks to protect the interests of another set of speakers—those whose content Verizon prefers to block—but has difficulty bringing them into the First Amendment analysis. And, lastly, listeners who seek out those speakers' content are likely not to count at all for constitutional purposes, even if they may be quite effectively censored by ISP decisions (for example, broadband consumers who live in an area served by only one provider, who decides to engage in blocking).

Taking greater account of listener interests raises at least two thorny problems: state action and balancing interests. The state action problem derives from the familiar (but not infrequently forgotten)[77] conclusion that the First Amendment checks only governmental restraints upon speech. Private entities such as publishers and distributors are free to speak or remain silent as they think best.[78] Listeners themselves are thus unlikely to have a constitutional claim against private intermediaries who limit their access to content.

76. Verizon Wireless, for example, initially refused to carry text (SMS) messages from NARAL Pro-Choice America, a group that advocates for abortion rights, but the company quickly reversed course. Adam Liptak, *Verizon Blocks Messages of Abortion Rights Group*, N.Y. TIMES, Sept. 27, 2007, at A1, *available at* http://www.nytimes.com/2007/09/27/business/27cnd-verizon.html.

77. *See, e.g.*, Jane C. Timm, *Republicans cry First Amendment after Duck Dynasty star's anti-gay rant*, MSNBC (last updated Sept. 3, 2014, 7:04 AM), http://www.msnbc.com/morning-joe/duck-dynasty-anti-gay-republican-defense (citing Louisiana governor's complaint that he "'remember[ed] when TV networks believed in the First Amendment'" after cable network A&E suspended a reality TV star for anti-gay comments).

78. There are rare exceptions, such as when a town owned by a private firm so closely resembled the state that it could be required to respect inhabitants' rights to freedom of speech and religion. Marsh v. Alabama, 326 U.S. 501 (1946).

However, the government should be able to advance listeners' interests when it regulates on their behalf, for example, by mandating that an intermediary carry content putatively desired by recipients, but to which the intermediary itself objects. If the intermediary challenges the regulation as an infringement of its speech—as Verizon has—the listeners' interests should count as part of the state's interest in the disputed statute. This differs in important ways from the usual rationale for must-carry or similar provisions. In cases such as right of reply for political candidates in newspapers, or requirements that cable television networks broadcast certain channels, the state's interest is typically defended as diversifying speakers rather than meeting listeners' demands. Diversification carries a risk of error; the government may be mandating inclusion of material (such as the public, educational, and governmental channels on cable television) that the audience perhaps ought to watch, but doesn't. By contrast, a listener-based framework should require that the government demonstrate some meaningful demand for the material subject to regulation. If Verizon ran afoul of network neutrality for blocking spam or phishing e-mails, the government would have trouble sustaining its burden. If the ISP blocked Netflix, or pornography, the government should have little trouble articulating listener demand.

The second, and harder, question is how a court reviewing this clash of interests—speaker faced with compelled speech, versus listeners faced with censorship—ought to weigh those competing claims. This sort of quasi-empirical weighting can be unsatisfactory; it's nearly impossible to compare interests meaningfully without a carefully established reference point. However, I wish to offer two proposals as candidates.

The first proposal focuses attention on listeners' alternatives. The impingement on listeners' rights diminishes as listeners have more options for broadband access. The analysis here should assess both the number of broadband providers and their practices; having more options serves listeners little if each provider implements similar restrictions. Courts should not fall into the trap of assessing an ISP's market power – that measures only part of the interests at stake.[79] A broadband provider with market power might implement a defensible restriction, or one that creates too little effect on listener interests to be cognizable. And, a provider that lacks market power might implement an unacceptable restriction, such as putting in place bandwidth-based constraints for streaming video, but only applying them to Netflix and not Amazon Instant. As consumers are increasingly able to switch among broadband

79. *Cf.* Verizon v. FCC, 740 F.3d 623, 659-68 (D.C. Cir. 2014) (Silberman, J., dissenting) (critiquing FCC's failure to evaluate market power of broadband providers).

providers with variegated policies on access to content, the basis for regulation—and hence its constitutionality—decreases.[80] Such an approach also preserves the possibility of innovation among access providers, such as family-friendly ISPs that block violent, pornographic, or other purportedly inappropriate content.

The second proposal evaluates the fit between the stated purpose for restricting communications and the implementation of that rationale. The greater the divergence—or, put another way, the less reliably the purpose is instantiated in practice—the less constitutional leeway afforded. One example from beyond U.S. borders comes from Vietnam's Internet censorship. Vietnam claims to implement restrictions on Internet content as a means of protecting minors from inappropriate content, such as pornography. However, while the country's ISPs block significant numbers of political and human rights Web sites, they do not block any pornographic sites. This divergence strongly suggests that Vietnam's purpose is pretextual, making its restrictions illegitimate. So, too, with restrictions put in place by U.S. providers. An ISP that purported to be concerned about bandwidth usage, but that blocked Netflix and not Hulu, or that blocked Google's home page, should be treated as encroaching unduly upon listener interests. Similarly, if Comcast should again degrade the performance of peer-to-peer software because of professed concerns over bandwidth, the company's treatment of other bandwidth-intensive applications or traffic should inform whether its restrictions are permissible.[81]

The transition to an all-IP world will upend First Amendment precedent that depends on technology or medium for its conclusions. And, a communications environment where previously different media simply become different applications will put pressure on the inchoate articulation of listener interests in free speech jurisprudence. Courts should move to take greater account of listeners—perhaps by assessing alternative channels, perhaps by evaluating intermediaries' justifications and implementation for restrictions. In any case, freedom to communicate in an all-IP world is a classic fox problem: it varies case-by-case, and eludes easy prediction.

80. This assumes that consumers treat broadband providers instrumentally – that they have no other normative basis for preferring, for example, Cox Cable to CenturyLink DSL. That assumption is plainly wrong in media such as newspapers or broadcast television, where carriage of content conveys implicit endorsement by the conduit. Given broadband providers' past practices of near common carriage, though, this imprimatur theory seems unlikely.

81. *See* Comcast Corp. v. FCC, 600 F.3d 642, 644-45 (D.C. Cir. 2010) (noting that "Comcast defended its interference with peer-to-peer programs as necessary to manage scarce network capacity.").

CONCLUSION

One must take the bitter with the sweet. The transition to an all-IP communications architecture brings problems as well as promise. The consolidation onto Internet Protocol risks reducing resiliency in the network, undercutting universal service commitments, and enabling greater private (and possibly public) censorship. And yet this change usefully forces us to think about why these challenges exist. Disaster planning, briefly in vogue after the 9/11 attacks, is now both vital and neglected. Universal voice service has become a mantra, rather than the embodiment of a carefully articulated commitment to communitarian values. And, media-specific First Amendment rules have fetishized the act of speaking rather than its goal: to persuade. A technological change that will be invisible to most Americans presses us to re-examine profound normative principles. Some of these questions are amenable to a single answer, even if difficult, and some must be answered in the context of their individual circumstances. Whether hedgehog or fox, these problems demonstrate the interweaving of technological and legal questions, and the opportunity that a change in the former presents to evaluate the latter.