Shortness of Vision: Regulatory Ambition in the Digital Age

Fordham Law Review

Volume 74 | Issue 2 Article 13

2005

Shortness of Vision: Regulatory Ambition in the Digital Age

Susan P. Crawford

PANEL V: RESPONSIBILITY AND LIABILITY ON THE INTERNET

SHORTNESS OF VISION: REGULATORY AMBITION IN THE DIGITAL AGE

*Susan P. Crawford**

INTRODUCTION

Quietly, in impenetrable regulatory language and carefully staged steps, some of the governments of the world have undertaken to constrain the open platforms and open devices that make up the network of networks that is the Internet. The Internet has matured and become vital to commercial life, they say, and surely it is time for someone to be in charge.[1] Meanwhile, public concern about the perceived dangers of online life is increasing. There is spam. There is spyware. There is pornography, and we will soon see more convulsive efforts to "protect" Internet users from its effects. Pummelled with news stories about the cesspools of online life, citizens who are not online may become less inclined to go there, and many of those who are merely sending email certainly wish that someone would make the spam go away. Meanwhile, the content industry and law enforcement authorities are both interested in constraining the free flows of information that have characterized the Internet so far. The convergence of regulatory ambition and public concern is unmistakable. It could well lead to actions that we will regret, as regulatory agencies take the occasion of

---

* Assistant Professor, Cardozo School of Law. Many thanks to Yochai Benkler, Michael Herz, David Johnson, Pam Samuelson, Kevin Stack, Stewart Sterk, and Tim Wu. An earlier version of this paper was discussed during the 2004 cyberprof retreat hosted by the Berkman Center for Internet and Society at Harvard Law School. Special thanks to Brianne Biggiani, Joshua Goldstein, and Anthony diFrancesca, who provided research assistance.

1. Interview with Markus Kummer, Head Secretariat of the United Nations Working Group on Internet Governance, Int'l Telecomm. Union, http://www.circleid.com/posts/interview_with_united_nations_head_secretariat_of_wgig/ (last visited Oct. 23, 2005).

> It is a positive sign that countries are discussing how to run the Internet, since it requires global solutions to its problems. . . . Governments now feel that the Internet has become so important that it should be regarded as a matter of national interest. And so they see the need for getting involved. . . . The governments who want to play a more active role also see a need for closer international cooperation. They feel that the United Nations is the natural system of global governance and they hold the view that a United Nations umbrella would be a prerequisite to give the necessary political legitimacy to Internet governance.

Id.

public fear to assert greater—but ultimately counterproductive—control over online applications and devices.

This global regulatory trend is sometimes referred to as the process of "Internet governance." My goal in this Article is to persuade you that we face a great choice in the current Internet governance debate between open platforms, open devices, and diversity, on the one hand, and constrained platforms, constrained devices, and monocultures, on the other. This is an important choice because of its implications for the value, richness, and vibrancy of all human communications. We should not take the evolutionary risky choice of imposing centrally controlled boundaries (or membranes) regulating flows of bits[2]—information—online. Moreover, if the proponents of centralized control are allowed to proceed, they will waste an enormous amount of energy working towards failure. While they may initially be emboldened to claim victory when their large-scale moves change the online landscape, over time the complexity of the Internet's information flows will defeat the forces of centralization. In the meantime, major opportunities for innovation, decentralized "regulation," and creative social and economic engagement will have been foreclosed.

Part I provides an analytical framework for the upcoming national conversation about governance of online information flows. The Internet is itself a complex adaptive system, made up of many interacting agents (including many non-state communities) whose dynamic engagements produce elaborate, decentralized, permeable membranes regulating information flow.[3] Think of the Internet as an environment in which government is attempting to operate, like the terrain on which a battle is played out. Where the complexity of a system (government) is insufficient to cope with the complexity of its environment (the Internet), the system will be unsuccessful. Although large-scale operations can defeat complexity when the large-scale system is able to operate (in the same way that a platoon of tanks can roll over a forest), if the large-scale system is

2. By "bits," I mean machine-readable representations of information. "Bit" is shorthand for "binary digit," the smallest unit of information on a machine. A single bit can exemplify only one of two values: 0 or 1. More significant information is obtained by combining consecutive bits into larger units—such as bytes, which are made up of eight consecutive bits. Netdictionary, http://www.netdictionary.com/b.html (last visited Oct. 23, 2005).

3. Other examples of complex systems are "[t]he economy, the stock market, the weather, ant colonies, earthquakes, traffic jams, living organisms, ecosystems, turbulence, epidemics, the immune system, river networks, land-slides, zebra stripes, sea-shell patterns, and heartbeats." Ben Moore, Inst. for Theoretical Physics, Univ. of Zurich, Complex Systems, http://krone.physik.unizh.ch/~moore/complex/complexity.html (last visited Oct. 23, 2005) (defining complexity). Interactions among the agents that make up a complex system lead to emergent properties of the system (properties that could not be explained by traditional analysis) that are not properties of the agents themselves. Complex networks have self-similar (fractal) properties, meaning that they consist of self-repeating patterns at all scales. Erica Klarreich, *Sizing Up Complex Webs: Close or Far, Many Networks Look the Same*, Science News Online, Jan. 29, 2005, http://www.sciencenews.org/articles/20050129/fob3.asp (reporting results from Chaoming Song et al., *Self-Similarity of Complex Networks*, 433 Nature 392 (2005)).

concerned about the fate of the complex structures it seeks to flatten, it will be unable to engage. There are many positive benefits of the Internet's complex information flows that governments will want to retain. Grappling with this complexity will ultimately make it impossible for governments to "govern the net."

Part II provides the domestic legal background for this battle. To date, the U.S. Congress has acted with great self-restraint in "regulating the Internet," with some exceptions. It has shielded platform providers from liability for the information flows they do not create, and has adopted relatively lightweight "notice and takedown" regimes for copyrighted materials inadvertently hosted or stored by platforms. It has refused to engage in special taxation systems for online commerce, and has (so far) not adopted special Internet data privacy laws. More recently, its obsession with sinful activities has led it to take aggressive (and aberrational) approaches to Internet gambling and "harmful to minors" online content. These incongruous steps have gotten Congress in trouble both globally and in the U.S. courts. In 2005, congressional self-restraint is under pressure, and this Article is an attempt to remind Congress of the correctness of its initial approach—and to strengthen congressional will to fend off the strident demands of law enforcement and the content industry for Internet regulation.

Two U.S. domestic case studies, both having to do with the powers of the Federal Communications Commission ("FCC" or "Commission"), demonstrate that agency's tendency to assume that a top-down engineering approach can "fix" online problems. The first, the broadcast flag rulemaking, focused on the interfaces between machines that manipulate digital content and the Internet.[4] The second, the IP-enabled services rulemaking,[5] concerns applications and services that use the Internet Protocol ("IP").[6] These two fascinating proceedings have largely gone unnoticed by the mainstream press, but are enormously important to the future of the Internet. They represent the first organized effort to "regulate the Internet" by creating centrally planned barriers to particular kinds of bits. Both of these proceedings have as their key goal the creation of mandated membranes (or boundaries) for information flows, by affecting what machines can send out online and what online applications can work on or provide. These proceedings ignore the possibility of any non-state sources of membranes—much less the idea that such membranes could evolve to shelter complex organisms of social order. They also conflict with the FCC's overall deregulationist approach to online issues and are

4. Digital Broad. Content Prot., 18 F.C.C.R. 23,550 (2003) (FCC report, order, and further notice of proposed rule).

5. IP-Enabled Services, 19 F.C.C.R. 4863 (2004) (FCC notice of proposed rulemaking).

6. The Internet Protocol ("IP") is "[t]he protocol used to route a data packet from its source to its destination via the Internet." Red Hat Glossary, http://www.redhat.com/docs/glossary/ (last visited Sept. 15, 2005).

likely outside the scope of the FCC's delegated powers. Thus, we will inevitably end up discussing these matters on Capitol Hill.

Part III tells the technical and political stories of these two rulemakings, and ties these proceedings to other world events that fall within the larger Internet governance category.

Part IV analyzes the legal tools that are available to understand and address this moment in the Internet's history, including available domestic constraints on the FCC's power. Congress has not given the FCC explicit statutory authority to act in either the broadcast flag or IP-enabled services situations. The FCC is relying on common-law "ancillary" jurisdiction, stemming from Title I of the Telecommunications Act,[7] as the source of its powers. In making rules that are legally binding on the public, however, an agency must be able to draw a line from its powers to some provision of enacted law.[8] No provision of existing law expressly supports (or even signals support for) the FCC's actions here, and Congress would not have delegated such economically important powers lightly.[9] Moreover, existing case law establishes that the FCC's ancillary jurisdiction is limited to acts that are necessary to ensure the achievement of the FCC's statutory responsibilities. Because there has been no showing in either of these settings that such necessity exists, it is likely that a court would find that the FCC does not have jurisdiction to impose the "social policy" rules stemming from the IP Notice of Proposed Rulemaking—just as a court has already found that the FCC did not have jurisdiction to impose the broadcast flag rule. Thus, we will need a national legislative conversation about the approach to the Internet embodied in these two rulemakings.

Part V then suggests an alternative outlet for governments' desires to constrain information flows. Governments will not be content with simply leaving information flows alone. Once we understand the importance of membranes and the impossibility of designing them in advance, governments' direction should be clear: They should act to encourage the evolution of decentralized feedback loops and membranes that can better do the job. Decentralization of choices about what is "good" (and, thus, what membranes for information flows are best) will lead, over time, to emergence of a clear path towards governance: evolution of complex organisms that will provide a constantly evolving, lively, and dynamic social order.

Who should be in charge online has become an extremely important cultural, social, and intellectual question. At this turning point in the

---

7. Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (codified as amended at 15 U.S.C. § 79z-5c and in scattered sections of 47 U.S.C.).

8. Thomas W. Merrill, *Rethinking Article I, Section 1: From Nondelegation to Exclusive Delegation*, 104 Colum. L. Rev. 2097, 2100-01 (2004) (discussing the importance of exclusive delegation understanding rather than nondelegation; agencies and courts have no inherent authority to make law (at least with respect to the matters covered by Article I), but Congress may transfer such authority to them) ("Article I, Section 1 tells us not that only Congress can legislate, but only Congress can delegate.").

9. FDA v. Brown & Williamson Tobacco Corp., 529 U.S. 120, 159 (2000).

development of the Internet, the need for longer-term and humbler collective vision is acute. We need to recognize that Internet governance is really about regulating information flows, that all we can hope to do globally is to encourage adequate evolution, and that finding someone to be the external pilot is both an impossible and dangerous task. In the absence of the long view, the world will suffer from the regulatory ambitions of central planners whose efforts are doomed to fail. We may never know what we have lost. The U.S. Congress should be encouraged to lead the world towards self-restraint, both because it is the right thing to do and because this approach will avoid expensively unsuccessful attempts to do otherwise.

I. PRINCIPLES OF NONREGULATION FOR THE INTERNET

Before taking on the question of membranes for information flows online, it is appropriate to review how the Internet differs from any other communications medium society has used to date. This will help ground the discussion of membranes and complex systems that follows.

The story of the Internet—and its exceptionalism—has often been told.[10] I set forth here only the briefest of summaries.

A. *What Is the Internet?*

The Internet is not a thing. It is an agreement to allow bits to flow among machines using a particular language, or protocol.[11] It is often thought of in terms of its layers—from bottom to top: (1) physical/infrastructure layer (cable, satellite, DSL, WiFi), (2) logical layer (TCP/IP, HTTP), (3) applications layer (browsers, email, Voice over IP ("VoIP")), and (4) content layer (speech, text, music).[12] The third and fourth layers are really not global layers at all. Instead, they are layers deployed by individuals and enterprises to make use of the lower layers. The first two layers separate transport (sending bits down a connection) from the protocol, such as TCP/IP, that chunks these bits into packets and allows them to be reassembled at the other end.[13]

---

10. For fine examples of writing about the architecture of the Internet and its interplay with law, see Lawrence B. Solum & Minn Chung, *The Layers Principle: Internet Architecture and the Law,* 79 Notre Dame L. Rev. 815 (2004); A. Michael Froomkin, *Habermas@Discourse.Net: Toward a Critical Theory of Cyberspace*, 116 Harv. L. Rev. 749 (2003); Mark A. Lemley & Lawrence Lessig, *The End of End-to-End: Preserving the Architecture of the Internet in the Broadband Era*, 48 UCLA L. Rev. 925 (2001).

11. William Gibson describes cyberspace as an immersive "consensual hallucination." William Gibson, Neuromancer 5 (1984).

12. Arguably, yet another layer is now evolving that facilitates the formation of complex social groups based on exchanges of bits and effective use of the metainformation that is generated by these exchanges. The emergence of this new "social protocol" layer of the Internet suggests that we will collectively build a better society, not just a better Internet, if we build systems and laws that let that society evolve online. That layer is the subject for another article.

13. *See* Webopedia Definition of TCP/IP, http://www.webopedia.com/TERM/T/TCP.htm (last visited Sept. 12, 2005).

The layers nondiscrimination principle dictates that all forms of the physical/infrastructure layer can or will permit the logical layer to run across them. Thus, fiber-optic infrastructure or wireless connections will permit TCP/IP to work. In turn, the logical layer, which contains the protocols that divide up packets and reconstruct them into messages or web pages, is not (in principle) supposed to discriminate against particular applications that use that logical layer. And applications are not (in principle) supposed to discriminate against particular forms of content.[14]

Implementation of the layers principle (e.g., not allowing the transport layer to discriminate against any of the three levels above) permits the end-to-end principle first articulated in an important paper by Jerome Saltzer, David Reed, and David Clark in 1984 to flourish.[15] The end-to-end principle suggests that communications—information—ideally should not be filtered or changed or operated on by the network itself, but only by the edges, at the level of client applications that individuals set up and manipulate.[16] This end-to-end principle, like the layers principle, keeps bits flowing freely across the lower levels of the protocol stack, to be processed only when they get much closer to the end user—the edge of the network.[17]

The miraculous growth of the Internet has in large part come from the nondiscrimination against higher levels that is part of the lower layers' architecture.[18] Innovators at the application layer have been able to assume

14. The layers concept has recently become a suggested model for regulatory intervention. In early 2004, MCI issued a paper suggesting that cable and telephone providers be required to make their networks available to others on a wholesale basis, citing (and relying on) the layers principle. Richard S. Whitt, Codifying the Network Layers Model: MCI's Proposal for New Federal Legislation Reforming U.S. Communications Law (2004) (MCI Public Policy Paper).

15. Jerome H. Saltzer, David P. Reed & David D. Clark, *End-to-End Arguments in System Design*, 2 ACM Transactions on Computer Systems 277 (1984).

16. *See also* David Isenberg, *Rise of the Stupid Network*, Computer Telephony, Aug. 1997, *available at* http://www.rageboy.com/stupidnet.html.

17. The openness of the Internet (rough nondiscrimination between layers, intelligence at the edges) stands in contrast to telephone networks, which use circuit switching. When a telephone call is made from one person to another, a dedicated connection is opened and sustained for the duration of the call. Because that connection goes in both directions, it is called a circuit. A call is routed via a local carrier through a switch to reach the person you are calling. Use of circuit switching therefore relies on intelligence—routing and processing decisions being made—residing at the center of the network. Indeed, a fundamental goal of telephony switches is to maintain control over circuits. *See* Susan P. Crawford, Someone to Watch over Me: Social Policies for the Internet (unpublished manuscript on file with author) (describing history of telephony). Data networks such as the Internet use packet-switching rather than circuit switching. There is no constant, open connection in a packet switched network. Instead, the sending computer divides data into packets, puts addressing information on each one, and opens a connection just long enough to send each packet one hop. The packets follow whatever route seems most efficient at the time (which may be different for each packet) and are reassembled by the receiving computer. Where a central telephone provider must provide enhanced functionalities at a physical termination point, IP network design is flat and highly decentralized, allowing substantial innovation to occur at the edges of the network. *Id.*

18. *See* Isenberg, *supra* note 16; *see also* ISOC: The Internet Society and Public Policy, http://www.isoc.org/news/3.shtml (last visited Oct. 23, 2005) ("The explosive growth of the

the continued stable existence of the lower layers, and have not had to provide for either transport or logical protocols in order to spread their applications.[19]

B. *Why Are Membranes Important to the Internet?*

The open standards and nondiscriminatory layers of the Internet have prompted much more than mere innovation. The Internet has given rise to an explosive growth in information flows, prompting the emergence of a richly varied, closely connected, and highly structured social, cultural, and intellectual online world. More than 900 million people are now online.[20] The world has become much smaller as a result of the Internet's growth; it is clear, for example, that the December 2004 tsunami relief response was spurred by Internet communications.[21] Blogs have replaced mainstream media as sources of news for many people.[22] Podcasting may replace radio.[23] These flows are not just one-to-many, however. Increasingly, we are seeing the emergence of a social layer of the protocol stack that involves group interactions of all kinds: one-many-few to one-many-few.[24] What makes this online structuring possible is the existence of membranes.

What is a "membrane"? For biological cells, of course, the membranes that surround them are vital. They define the cell and determine what it can and cannot do. Membranes were the first structures of living organisms to

---

Internet and the incredible variety of Internet applications are a direct result of the fact that the key standards for the Internet and the Web are open.").

19. *See* ISOC: The Internet Society and Public Policy, *supra* note 18.

20. ClickZ Stats Web Worldwide, Trends & Statistics: The Web's Richest Source, http://www.clickz.com/stats/web_worldwide/ (last visited Oct. 23, 2005).

21. As David Ho reported,

> Rapidly changing estimates on the amount raised for victims of the Southeast Asian earthquake and tsunami vary greatly, but there is consensus that at least half of the hundreds of millions in private donations arrived through the Internet. The American Red Cross has raised more than $168 million with more than $71 million coming through its Web site, according to The Chronicle of Philanthropy. Of the $35 million received by the U.S. Fund for UNICEF in New York, $25 million is in Internet donations.

David Ho, *Record Online Tsunami Relief Changes Ways of Giving*, The Fin. Express, Jan. 17, 2005, http://www.financialexpress.com/fe_full_story.php?content_id=79947?headline=Record~online~tsunami~relief~changes~ways~of~giving.

22. Lee Rainie, Pew Internet & American Life Project, The State of Blogging (2005), http://www.pewInternet.org/pdfs/PIP_blogging_data.pdf (finding that blog readership was up fifty-eight percent in 2004, that six million Americans get news and information fed to them through Rich Site Summary ("RSS") aggregators, but that sixty-two percent of Americans were unsure, however, of what a "blog" was).

23. Daniel Terdiman, *Podcasts: New Twists on Net Audio*, Wired News, Oct. 8, 2004, http://www.wired.com/news/digiwood/0,1412,65237,00.html.

24. Beth Simone Noveck, A Democracy of Groups 3-4 (2005) (unpublished manuscript, on file with the author) ("[T]echnology is revolutionizing our capacity for purposive collective action with geographically remote actors. . . . This evolution toward technology for groups is evident from Meetups, Wikis, LiveJournal, peer-to-peer, groupware, virtual worlds, GRID computing, [and] a wide range of so-called "social software" tools, such as Friendster or Wallop.").

evolve,[25] and their basic function is to separate the inside from outside—to separate the chemicals and structures needed to maintain the cell from the outside environment. Membranes regulate in both directions, filtering what comes in and what goes out. The properties of cell membranes arise from the physical behavior of various lipids (water-insoluble substances). Bacteria can be destroyed by antibiotics punching holes in their cell membranes, making them porous and leaky.[26] All membranes are permeable, but you can have too much of a good thing. Some membranes also have a homeostatic function in that they protect what is inside from rapid change; not from all change, which would be deadly, but from too much change too quickly.[27]

There have always been membranes for information flows, and we have always created them in decentralized ways. Every time an individual or a group decides not to listen to some outside source of information, allows a new member in, or reads something suggested by a colleague, he/it is using (and participating in constructing) a permeable membrane. For cells and other living things, permeable membranes are nutrient collection and drop-off areas; for minds, permeable membranes are information collection and rejection areas that help us select the right data from the constant and overwhelming flows surrounding us. Informational membranes are everywhere, and no one has to tell us how to create them or what their characteristics are. There is no one "in charge" of this structure.

How do permeable informational membranes operate online? The swapping of information is a simple interaction, but it requires copying onto some substrate or surface in order for the information to continue to exist and replicate and (eventually) evolve. For a bit, the best way to travel is to be replicated or to be sent, as a copy, somewhere. So membranes for bits are predominately established by the availability of mechanisms that allow or frustrate the ability to make or send copies. Many online membranes are very simple: who is allowed to be a member of a particular listserv, how do you leave a particular provider of online services, what content is appropriate for what online site, what community of blogs links to one another, and more. Increasingly, online information is subject to the membrane of attention. Some people (or some groups) pay attention to a particular kind of information flow (and in so doing are directing whatever membrane they have adopted to take in—be permeable to—this information). We are remarkably selective about what we will take on board and what we will not.

The growth of the Internet, through the networked, interactive screens that make it human-readable, has facilitated a wild proliferation of

25. McGraw-Hill Online Learning Center, The Importance of Membranes, http://highered.mcgraw-hill.com/sites/0073031216/student_view0/exercise9/the_importance_of_membranes.html (last visited Sept. 10, 2005).

26. Lukas Buehler, *What Is Life*, http://www.whatislife.com/education/fact/history.htm (last visited Sept. 7, 2005).

27. *See* Definition of Homeostasis, WordReference.com Dictionary, http://www.wordreference.com/definition/homeostasis (last visited Oct. 23, 2005).

interestingly permeable membranes. These membranes, in turn, have facilitated a wild proliferation of varied information flows. The conceptual and code-based rules that surround these communities act as two-way membranes, permitting and prohibiting the flow of bits. These membranes are legal code in the Lawrence Lessig sense,[28] but to describe them as "law" would miss most of their important features. They are also the means by which individuals and groups govern dialogue, communication, flux, and flow. What we pay attention to defines who we are.

Government has not previously attempted to regulate who we are by way of mandated information flow membranes, or at least not successfully. Governments make disclosure rules that require the display of information, like nutritional labeling, credit disclosures, and product safety statements. But these are very different from mandated creation of membranes (e.g., "this kind of information may not pass through this kind of barrier.") We have rarely allowed governments to establish or control informational membranes.[29] Nor have we ever had to be explicit about the source of informational membranes, because it was self-evident that offline information flows were matters of nongovernmental decision. Membranes are fundamental, emergent entities, existing only as a property of the collective organism that created them. Centralized attempts to change or ban particular informational membranes, such as mandating the use of official languages,[30] or requiring that particular words not be used,[31] feel to

28. *See generally*, Lawrence Lessig, Code and Other Laws of Cyberspace (1999).

29. Obscenity and child pornography, of course, are exceptions to this rule. But child pornography laws are arguably focused on avoiding abuse of children rather than prohibiting communication of information that appears to depict children engaged in sexual activities—behavior, rather than communication, is the true target of these laws. *See* Ashcroft v. Free Speech Coal., 535 U.S. 234 (2002) (holding unconstitutional a ban on virtual child pornography). Federal Communications Commission ("FCC") rules regulating "indecent" and "profane" broadcast content (by limiting such content to broadcast between 10:00 pm and 6:00 am), 47 C.F.R. § 73.3999 (2004); *see* 18 U.S.C. § 1464 (2000), seem increasingly anachronistic. As Professor Michael Dorf of Columbia said not long ago, "Was the [Janet Jackson] halftime show unsuitable for the millions of small children watching? Sure. But so are half the shows on prime-time television." Michael Dorf, *Does the First Amendment Protect Janet Jackson and Justin Timberlake*, CNN.com, Feb. 4, 2004, http://www.cnn.com/2004/LAW/02/04/findlaw.analysis.dorf.jackson.indecency/. Nearly 100 percent of the indecency complaints sent to the FCC in 2003 stemmed from a single advocacy group—the Parents Television Group. Todd Shields, *Activists Dominate Content Complaints*, MediaWeek.com, Dec. 6, 2004, http://www.mediaweek.com/mediaweek/headlines/article_display.jsp?vnu_content_id=1000731656. In *Reno v. ACLU*, 521 U.S. 844 (1997), the Supreme Court struck down an indecency standard for the Internet. Rules restricting online gambling also appear to be anachronistic at this point.

30. *See generally* James Crawford, Hold Your Tongue: Bilingualism and the Politics of 'English Only' (1992).

31. "As French culture [and language have] come under increasing pressure with the widespread availability of English media, the Académie [Française] has tried to prevent the anglicisation of the French language." Wikipedia, Académie Française, http://en.wikipedia.org/wiki/French_academy (last visited Oct. 23, 2005). It is as a direct result of a decision of the Académie that the French word for "computer" is "ordinateur" and that the field of study dealing with computers is known as "informatique" (informatics), from the contraction of "information" and "automatique." *Id.*; *see also* David G. Post, *"The*

us like thought control. Individuals are likely to reject such centralized filtering attempts.

Governments can, of course, act on atoms. Governments create enforceable barriers and borders and speed limits that affect behavior. We will respond to force when it is used to compel us to modify our actions, and we have entire systems of criminal justice that are based on this premise. But shaping a road barrier, mandating a speed limit, or requiring a nutritional disclaimer are all governmental acts that are entirely different from requiring that boundaries to information flows be erected and maintained.

II. CONGRESS AND "REGULATING THE INTERNET"

The United States claims pride of place as the inventor of the Internet, and it is beyond question that U.S. government funding (and interoperability requirements) made the Internet possible. How has the U.S. Congress dealt with the complexities of information flow membranes online?

A. *The Hands-Off Approach*

The clearest statement of Congressional purpose when grappling with Internet information flows is found in Section 509 of the Telecommunications Act of 1996, 47 U.S.C. § 230:

> (a) FINDINGS. The Congress finds the following: (1) The rapidly developing array of Internet and other interactive computer services available to individual Americans represent an extraordinary advance in the availability of educational and informational resources to our citizens. . . . (4) The Internet and other interactive computer services have flourished, to the benefit of all Americans, with a minimum of government regulation. . . .
>
> (b) POLICY. It is the policy of the United States . . . (2) to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation . . . .[32]

In this section, Congress explicitly elected not to impose common carrier obligations (regulating content, prices, or access by others) on interactive computer services. Prior to the enactment of § 230, interactive and computer service providers faced fearsome potential liability for content created by third parties because of two key (and inconsistent) court decisions.[33] Congress listened to the concerns of interactive service

---

Free Use of Our Faculties": Thomas Jefferson, Cyberspace, and the Languages of Social Life, 49 Drake L. Rev. 407 (2001).

32. Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56, 137-39 (codified as amended at 47 U.S.C. § 230 (2000)).

33. Cubby, Inc. v. CompuServe, 776 F. Supp. 135 (S.D.N.Y. 1991); Stratton Oakmont, Inc. v. Prodigy Servs. Co., No. 31063/94, 1995 N.Y. Misc. LEXIS 229 (N.Y. Sup. Ct. Nassau Cty. May 24, 1995).

providers and enacted § 230 to protect them from liability for content created by others so as to avoid hampering online service innovation. As the Fourth Circuit held in *Zeran v. America Online, Inc.*,[34] "[b]y its plain language, § 230 creates a federal immunity to any cause of action that would make service providers liable for information originating with a third-party user of the service."[35] Since its adoption, § 230 has been construed to establish almost universal immunity for service providers that are sued based on content created by third parties.[36] § 230 was enacted to support the robust nature of Internet communication and to keep government interference in information flows to a minimum.[37] Illegal speech (defamation, obscenity, copyright infringement) continues to be illegal, but is primarily targeted as a behavior of individual humans rather than at the membrane level through governmental stemming of particular flows of data across platforms or technologies.

Congress has continued to legislate in the spirit of § 230. For example, the Internet Tax Freedom Act[38] has imposed moratoriums since 1998 (now extended to 2007) on state and local taxes on Internet access and multiple or discriminatory taxes on e-commerce.[39] The Digital Millennium Copyright Act ("DMCA"),[40] although rightfully criticized for its broad restrictions on circumventing copy protection technology,[41] enshrines a deal that protects online service providers from liability for copyright infringement by users if

34. 129 F.3d 327 (4th Cir. 1997).

35. *Id.* at 330.

36. *See* Ben Ezra, Weinstein & Co. v. Am. Online, Inc., 206 F.3d 980 (10th Cir. 2000); Doe v. Franco Prods., No. 96-4095, 2000 U.S. Dist. LEXIS 8845 (N.D. Ill. June 22, 2000), *aff'd on other grounds*, 347 F.3d 655 (7th Cir. 2003); Blumenthal v. Drudge, 992 F. Supp. 44 (D.D.C. 1998); *cf.* Barrett v. Rosenthal, 9 Cal. Rptr. 3d 142 (Cal. Ct. App.) (ruling by California lower court that section 230 immunity does not apply when the individual republishing the statements knew or had reason to know of the falsity of the material being disseminated), *petition for review granted and opinion superseded by* 87 P.3d 797 (Cal. 2004).

37. Zeran v. Am. Online, Inc., 129 F.3d 327, 333 (4th Cir. 1997), *cert. denied*, 524 U.S. 937 (1998). As the *Zeran* court explained,

> More generally, notice-based liability for interactive computer service providers would provide third parties with a no-cost means to create the basis for future lawsuits. Whenever one was displeased with the speech of another party conducted over an interactive computer service, the offended party could simply "notify" the relevant service provider, claiming the information to be legally defamatory. In light of the vast amount of speech communicated through interactive computer services, these notices could produce an impossible burden for service providers, who would be faced with ceaseless choices of suppressing controversial speech or sustaining prohibitive liability. Because the probable effects of distributor liability on the vigor of Internet speech and on service provider self-regulation are directly contrary to § 230's statutory purposes, we will not assume that Congress intended to leave liability upon notice intact.

Id.

38. Internet Tax Freedom Act, 47 U.S.C. § 151 note (2000).

39. Internet Tax Nondiscrimination Act, Pub. L. No. 108-435, 118 Stat. 2615 (2004) (to be codified at 47 U.S.C. § 609 note).

40. Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (1998) (codified in scattered sections of 17 U.S.C. and at 28 U.S.C. § 4001).

41. *See, e.g.*, Dan L. Burk, *Anticircumvention Misuse*, 50 UCLA L. Rev. 1095 (2003).

the provider "expeditiously" removes the infringing material after receiving notification from the copyright owner.[42] And Congress has to date not adopted a widely applicable online privacy law, preferring instead to take a sectoral approach—grappling with financial privacy[43] and health privacy[44]—that applies to both offline and online data.[45]

B. *The Intermeddling Approach*

Congressional and prosecutorial efforts to regulate online information flows by mandating that particular membranes or barriers be put in place have been met with prolonged litigation and—mostly—have not survived constitutional scrutiny. Congressional obsession with pornography led to the Communications Decency Act ("CDA"), which would have prohibited posting "indecent" or "patently offensive" materials in a public forum online.[46] The CDA was declared unconstitutional in a landmark U.S. Supreme Court decision in 1997.[47] The Child Online Protection Act ("COPA") was then enacted into law in 1998,[48] and would have prohibited commercial website operators from offering material that was suitable for adults but considered "harmful to minors" unless such sites verified the age

42. 17 U.S.C. § 512 (2000).

43. Gramm-Leach-Bliley Financial Modernization Act, 15 U.S.C. § 6801 (2000).

44. Health Insurance Portability and Accountability Act, Pub. L. No. 104-91, 110 Stat. 1936 (1996) (codified in scattered sections of 18, 26, 28, and 42 U.S.C.).

45. Its one excursion into a specialized online privacy law, the Children's Online Privacy Protection Act, 15 U.S.C.A. § 6503 (2004), has not been a success; many sites have elected simply not to provide interactive services for children under thirteen rather than cope with the exacting oversight and notice requirements of the Act. *See* Carrie Kirby, *Youth Privacy Net Law Takes Effect, Many Web Site Operators Worry They'll Lose Money on Children's Market*, S.F. Chron., Apr. 21, 2000, at B1, *available at* http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2000/04/21/BU102542.DTL &type=business); Ben Charny, *The Cost of COPPA: Kids' Site Stops Talking*, ZDNet, Sept. 12, 2000, http://news.zdnet.com/2100-9595_22-523848.html?legacy=zdnn. A report by the Electronic Privacy Information Center also noted that

> [c]ritics have claimed that the methods outlined by the [Federal Trade Commission ("FTC")] for verification—sending/faxing signed printed forms, supplement of credit card numbers, calling toll-free numbers, or forwarding digital signatures through email—are too costly, cumbersome, and inadequate in protecting personal information. Even though new technologies are being developed, the current verification methods are too slow and impractical. The process of verification of mails, emails, and credit card numbers may take over a day. Further, disclosure of credit card information will expose the parents to the same privacy risks that they are trying to protect their children from and deter them from using such online services in general. As a consequence, children may manipulate information to access these websites, and in the long run, online businesses may . . . eliminate children-focused sites.

Electronic Privacy Information Center, The Children's Online Privacy Protection Act (COPPA), http://www.epic.org/privacy/kids/ (last visited Sept. 2, 2005).

46. Communications Decency Act, 47 U.S.C. § 223 (2000).

47. Reno v. ACLU, 521 U.S. 844 (1997).

48. Pub. L. No. 105-277, 112 Stat. 2681 (1998) (codified as amended at 47 U.S.C. § 231 (2000)).

of all visitors. After several years of litigation, the Supreme Court in June 2004 enjoined the enforcement of COPA.[49]

The next information-flow membrane mandate to pass Congress—again, prompted by legislators' fixation on indecent (but legal) content online—was the Children's Internet Protection Act ("CIPA"),[50] which required libraries to install filtering software on all their computers capable of accessing the Internet in order to hold on to their federal funding. The goal of this 2000 legislation was to condition provision of such funding on libraries' use of filters that block access to visual depictions that are harmful to minors (when accessed by a minor). On June 23, 2003, after another three years of litigation, the Supreme Court upheld CIPA, with two "swing" Justices (Anthony Kennedy and Stephen Breyer) suggesting that adults would be able to ask librarians to unblock legal sites (legal for adult viewing, if harmful to minors) that had been blocked by the installed filters.[51] Even though the tie to the CDA was clear—this was another congressional attempt to eliminate online sexual material using technology that would also inevitably filter out protected speech—the link to federal funding made this case one the Justices could decide differently.[52] Indeed, the federal funding element may have been the crucial difference between CDA and CIPA. One European commentator noted the CIPA opinion as an "important shift" by an American legal system that had been "previously critical of government's attempts to regulate Internet access."[53]

Not only has Congress drawn an enormous amount of litigious energy with its aberrational attempts to pass categorical laws about information flows online, the global trade reputation of the United States is also being affected. Recently, the World Trade Organization ("WTO") has challenged U.S. decisions to declare online gambling by U.S. citizens illegal, claiming that these restrictions violate trade promises that the United States has made.[54] The United States interprets the 1961 amendments to 18 U.S.C. §

---

49. The Court sent the case back down for a trial to evaluate whether technology had changed in the intervening five years since the law was first declared unconstitutional by the Third Circuit. *See* Ashcroft v. ACLU, 540 U.S. 1072 (2003).

50. Pub. L. No. 106-554, 114 Stat. 2763 (2000) (to be codified at 20 U.S.C. § 7001).

51. United States v. Am. Library Ass'n, 539 U.S. 194 (2003).

52. Justice William Rehnquist, writing for the majority, noted that "Congress has wide latitude to attach conditions to the receipt of federal assistance in order to further its policy objectives. . . . We have held in two analogous contexts that the Government has broad discretion to make content-based judgments in deciding what private speech to make available to the public," and stated that categorical content controls were appropriate in the dynamic context of the Internet. *Id.* at 203-04.

53. Marcus Alexander, Filtering the Public Forum, CMLP Self Regulation Review (June/July 2003), http://www.selfregulation.info/iapcoda/0307xx-selfregulation-review.htm.

54. *See* James D. Thayer, *The Trade of Cross-Border Gambling and Betting: The WTO Dispute Between Antigua and the United States*, 2004 Duke L. & Tech. Rev. 0013, http://www.law.duke.edu/journals/dltr/articles/2004dltr0013.html; *House of Cards; The WTO and Online Gambling*, The Economist, Nov. 18, 2004, at 28, *available at* http://www.economist.com/business/displayStory.cfm?story_id=3411641; The Associated Press, *WTO: U.S. Should Drop Online Gambling Ban*, newsfactor.com, November 11, 2004, http://www.newsfactor.com/story.xhtml?story_id=28343.

1084,[55] written to address betting on sports over the telephone, to cover online gambling, and some site operators in the U.S. have been prosecuted under this interpretation. Antigua had argued to the WTO that the U.S. was providing half of the world's customers for online gambling services, despite the illegality of this activity under United States law. At the same time, Antigua had "sought to provide gambling and betting services to the United States," but the U.S. had condemned such services as illegal.[56] Under an exception to the WTO's General Agreement on Trade in Services ("GATS"), members are permitted to adopt measures that are "necessary to protect public morals" even if they do not meet "market access" or "national treatment" standards of GATS, and the U.S. has argued that its position with respect to gambling fits within this exception.[57] So far, the WTO has dismissed this "public morals" argument, perhaps because online gambling is so easily available in the U.S.

More recently, the U.S. effort to regulate email information flows through requiring accurate header information in emails and opt-out procedures has met with ridicule around the world.[58] The U.S. is not alone in this legislative failure. Most legislative measures—in the United States, Europe, and Australia—have had little impact on the spam problem.[59]

---

55. Pub. L. No. 87-216, 75 Stat. 491 (codified at 18 U.S.C. § 1084).

56. Thayer, *supra* note 54, at ¶ 2 (citing First Written Submission of Antigua and Barbuda, United *States—Measures Affecting the Cross-Border Supply of Gambling and Betting Services*, WT/DS285 (Oct. 1, 2003)); *see also* BBC, *WTO Rules Against U.S. Gambling Ban*, Nov. 11, 2004, *available at* http://news.bbc.co.uk/2/hi/business/4001793.stm.

57. General Agreement on Trade in Services, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex IB, Legal Instruments—Results of the Uruguay Round, 33 I.L.M. 1225, 1168 (1994). The U.S. Trade Representative, Robert Zoellick, has said about this exception, "If this isn't an exception that they should meet, I don't know what is." Thayer, *supra* note 54, at 8 (quoting *WTO Gambling Decision "deeply flawed"*, Reuters, March 25, 2004).

58. Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 ("CAN-SPAM"), Pub. L. No. 108-87, 117 Stat. 2699 (to be codified at 15 U.S.C. §§ 7701-13 and 18 U.S.C. § 1037); *see* Tom Zeller, Jr., *Law Barring Junk Email Allows a Flood Instead*, N.Y. Times, Feb. 1, 2005 at A1 ("A year after a sweeping federal antispam law went into effect, there is more junk e-mail on the Internet than ever.... A survey from Stanford University in December showed that a typical Internet user now spends about 10 working days a year dealing with incoming spam."). In a January 2004 press release, Spamhaus also noted that

> [a]gainst the advice of all anti-spam organizations, the U.S. House of Representatives has passed the CAN-SPAM Act, a bill backed overwhelmingly by spammers and dubbed the "YOU-CAN-SPAM" Act because it legalizes spamming instead of banning it.... From December 11, spamming will be illegal in the UK, but with 90% of the UK's spam problem originating in the United States, British users will continue to be flooded, now with 'legal' spam from the U.S.

Press Release, Spamhaus, United States Set to Legalize Spamming on January 1, 2004 (Nov. 22, 2003), http://www.spamhaus.org/news.lasso?article=150.

59. Postini, Inc., Annual Report (2005), http://www.postini.com/whitepapers/?WPID=25. This report noted that even as attention to the cost and prevention of spam reached a high point in 2004, threats to email systems grew worse as the incidence of spam remained at seventy-five to eighty percent of email, virus attacks grew threefold, and directory harvest attacks ("DHA") continued to plague corporate email servers. *See generally id.* For a discussion of how peer governance could fix spam,

These examples of U.S. efforts to regulate online information flows and membranes are only illustrative; an exhaustive treatment of this subject is beyond the scope of this Article. My argument is this: Congress took the right approach, the approach supporting the further growth of the Internet, in § 230 and in the Internet Service Provider ("ISP") liability sections of the DMCA. When, more recently, its absorption with pornography has led it to attempt to lock down information flows online, it has faced enormous litigation burdens (CDA, COPA, CIPA) and has achieved little success—either because the laws have been struck down as unconstitutional or because they have had little impact on the ground. More fundamentally, these efforts are hopelessly inadequate to deal with the scale of the complex information flows present in the online world.

III. CASE STUDIES: TWO FCC PROCEEDINGS

Notwithstanding the inherent difficulty of regulating information flows, steps are being taken worldwide by governments to constrain the openness of the Internet and the devices that connect to this network of networks. In this regard, the telecommunications and other agencies that form part of national governments are largely ahead of the legislatures in their countries. In particular, congressional reluctance to "regulate the Internet" in the U.S. is being overtaken by the eagerness of the FCC to expand its jurisdictional turf and maintain its relevance in the digital age.

In this part, I focus on two efforts being made by the FCC to (1) constrain the functioning of digital devices (the broadcast flag proceeding) and (2) constrain the layer-independence and end-to-end nature of the Internet (the IP-enabled services proceeding). These two proceedings are at different stages of maturity. The broadcast flag rule has been struck down by the United States Court of Appeals for the D.C. Circuit on jurisdictional grounds, and legislation may be introduced to grant the Commission clear jurisdiction to reissue the rule. Early indications from the IP-enabled services rulemaking are that broad rules will emerge from the Commission.

A. *Broadcast Flag Background*

The broadcast flag is beautifully and effectively named, because it is neither about broadcast nor limited to the waving of a patriotic "flag." Indeed, those who learn about the broadcast flag scheme quickly forget that it is focused on protecting digital television broadcasts and speak generally about the protection of digital content. And the "flag" is, in a sense, the least important part of the entire scheme.

Let's begin at the beginning. The flag is a set of bits embedded in a digital stream (a standard adopted by the Advanced Television Systems Committee ("ATSC") that signals "the bits following this set of bits are to

---

spyware, and other online ills, see David R. Johnson et al., *The Accountable Internet: Peer Production of Internet Governance*, 9 Va. J.L. & Tech. 9 (2004).

be protected."[60] The flag is itself a very simple signal. It is the implementation of the flag that matters.

The broadcast flag rule,[61] distilled to its essence, is a mandate that all consumer electronics manufacturers and information technology companies ensure that any device that touches digital television content "recognize and give effect to" the flag by protecting content against unauthorized onward distribution. The FCC claimed that the rule would protect digital television ("DTV") broadcasts from massive redistribution over the Internet.

The key reason for the adoption of the broadcast flag was the studios' (not the broadcasters') worries about the "Napsterization" of their content.[62] The threat of digital redistribution is particularly acute for movie studios and other video content producers because their business models are today highly dependent on repurposing programming. The current movie studio business model is based on studios' ability to exploit multiple distribution streams for each work they produce. Licensing and distribution agreements for these windows (domestic and international box office, airline performances, pay-per-view, rental, home sale, satellite, premium and basic cable, over-the-air broadcast, etc.) result in payment to the studios. If key (expensive) content files can be found "in the wild," online, the studios' fear is that no one will pay for them.

In order to avoid this "Napsterization," the FCC established a new, controversial, and extraordinarily broad regulatory regime that mandated the use of "authorized" content protection technologies by virtually every consumer electronics product and computer product—including digital television sets, digital cable set-top boxes, direct broadcast satellite ("DBS") receivers, personal video recorders ("PVRs"), DVD recorders, D-

60. Advanced Television Sys. Comm., ATSC A/65B: Program and System Information Protocol for Terrestrial Broadcast and Cable (2003), *available at* http://www.atsc.org/standards/a_65b.pdf. This standard defines the way that broadcasters must include program name and content information in TV broadcasts. The Advanced Television Systems Committee standard defines a "redistribution control" parameter. *Id.* at 78-79. This is the "broadcast flag" to which receivers of television signals, including PCs with tuner cards, must adhere.

61. Digital Broad. Content Prot., 18 F.C.C.R. 23,550 (2003) (FCC report, order, and further notice of proposed rule).

62. "Napsterization" is shorthand for the music industry's claim that rampant online file trading has led to a substantial diminution in revenues.

> The threat [to Hollywood executives] is the specter of a new Napster-like sensation that would make it easy for Internet users to bypass the studios and to view and swap movies for free. No service with such wide appeal looms—yet—but studio executives have been studying the music industry's experience with file-swapping services such as Napster. And while no one will say it out loud, privately they admit they're terrified Hollywood will be Napsterized: that some college kid will post a movie-swapping program that will explode in popularity, swiftly creating a ravenous audience of millions of users who will expect free access to Hollywood blockbusters.

Laura Rich, *Analysis: Hollywood Braces for 'Napsterization,'* CNN.com, Jan. 10, 2001, http://archives.cnn.com/2001/TECH/computing/01/10/hollywood.napsterization.idg/.

VHS recorders, and computers with tuner cards.[63] Specifically, the order required that all devices or software manufactured after July 2005 that could receive TV signals (including personal computers ("PCs") equipped with a tuner card) (1) check for the presence of the flag, (2) store and record flagged content using "authorized technologies," and (3) allow transmissions through digital interfaces (and only protected digital interfaces) only to other devices that had an approved copy-protection system installed.[64] As a practical matter, this meant that the flagged digital content would thereafter be blocked from distribution (1) to any other electronic device (like a cell phone or PC or DVD recorder) unless that device was itself compliant with the flag scheme, or (2) over the Internet.[65] In other words, a membrane was mandated by the FCC: "[T]hese kinds of bits shall not pass through this barrier."

Until the FCC could settle on a new regime for approval of "authorized" technologies, it itself decided (with a great deal of input from the content industry) which copy protection technologies manufacturers would be allowed to use.[66] The FCC's process blocked many proposed new uses of digital television content that involved transmission over the public Internet.[67] Of the thirteen proposed technologies, at least four originally included plans for allowing limited transmissions of encrypted flagged content over the Internet to a specified group of people.[68] Following objections from the Motion Picture Association of America ("MPAA") made to the FCC, three of those companies agreed to drop their Internet-related plans.[69] Thus, all of the approved technologies, save one, prohibited transmission over the public Internet of flagged content. TiVoGuard, the lone holdout against the MPAA's forceful demands to the FCC that all thirteen technology providers revise their plans, itself permitted

63. The rule provided that a digital TV demodulator manufactured after July 2005 could not lawfully send unprotected (unencrypted) content to any output, except in a set of specific cases: (1) as analog output (at least until the FCC closes the "analog hole"); (2) through specific digital output formats which must maintain the presence of the broadcast flag and are protected by an "Authorized Digital Output Protection Technology;" or, (3) in encrypted form, to devices that also follow the broadcast flag rules. *See Digital Broad. Content Prot.*, 18 F.C.C.R. at 23,589.

64. *See id.*

65. *Id.*

66. Digital Output Prot. Tech. & Recording Method Certifications, 19 F.C.C.R. 15,876, 15,907 (2004) (FCC order); Certifications for Digital Output Prot., Tech. & Recording Methods to be Used in Covered Demodulator Prods., 19 F.C.C.R. 4732 (2004) (FCC public notice).

67. Ctr. for Democracy & Tech., All Eyes on TiVo: The Broadcast Flag and the Internet (2004), *available at* http://www.cdt.org/copyright/ 20040726tivoflag.pdf.

68. These four are Thomson's SmartRight Technology, RealNetworks's Helix DRM Trusted Recorder, Microsoft's Windows Media Digital Rights Management Technology, and TiVo's TiVo Guard proposal.

69. All save TiVo agreed to insert "time to live" ("TTL") and "round trip time" ("RTT") limitations in the packets generated by the protection technology. These limitations mean that packets can travel no more than three hops (in no more than seven milliseconds) before expiring—so they will not get very far. *See Digital Output Prot. Tech. & Recording Method Certifications*, 19 F.C.C.R. at 15,907.

transmissions only to a single computer with a "dongle" (a small device that plugs into a computer port that prevents illicit copies of software from being made) attached or within a constrained personal network.[70] The broadcast flag scheme thus had an extraordinarily broad scope. It created a whole new regime of constraining regulation all at once: restrictions on Internet use; design mandates for consumer electronic equipment, including the traditionally open-platform PC; and licensing requirements for any device that connects to the regulated device. Unpredictable, amplifying, and possibly conflicting results from these downstream effects were likely to follow (and may still follow if Congress authorizes the Commission to readopt the order).

In the course of defending its authority to regulate equipment manufacturers in order to effectuate the flag scheme, the FCC broadly asserted that it had had jurisdiction since 1934 over any device that was "*associated with* the overall circuit of messages sent and received over all interstate radio and wire communication."[71] In other words, FCC claimed that anything that had some relationship with a U.S. wire or radio communication was subject to its design authority. This breathtaking—and, as the D.C. Circuit found, illegal—assertion swept within its boundaries all computers, car radios, VCRs, portable music devices, and bedside alarm clocks. Although the Commission conceded that this was the first time it had exercised such jurisdiction over equipment manufacturers, it claimed that "the nation now stands at a juncture where such exercise of authority is necessary."[72]

B. *The Flag and Membranes*

Although the broadcast flag proceeding nominally targeted receivers of television broadcasts, and thus appeared to have limited impact on the rest of the world of machines—particularly because more than eighty-five percent of Americans receive television broadcasts through cable and satellite connections that are subject to different rules[73]—its actual scope was much broader. Our PCs and televisions now collaborate to store and display live TV, movies, music, videos, and photos across broadband connections and within home networks. We are all using digital cameras,

---

70. *Id.* at 15,887.

71. Brief for Respondents at 17, Am. Library Ass'n v. FCC, 406 F.3d 689 (D.C. Cir. 2005) (No. 04-1037).

72. *Digital Output Prot. Tech. & Recording Method Certifications*, 19 F.C.C.R. at 15,889.

73. *See, e.g.*, University of Pennsylvania: Research at Penn: Business: Television's Digital Dilemma (Aug. 28, 2002), http://www.upenn.edu/researchatpenn/article.php?427&bus. As for digital cable and satellite TV, the content industry made a direct deal with cable and satellite broadcasters to impose content protection controls on all future television devices. The resulting negotiated rules were approved as part of the "Plug & Play" proceeding that facilitated the direct connection of digital navigation devices or other customer premises equipment to cable television systems. *Commercial Availability of Navigation Devices & Compatibility Between Cable Sys. & Consumer Elec. Equip.*, 68 Fed. Reg. 35,818 (Jun. 17, 2003).

camcorders, and phones that behave like cameras. No manufacturer of any one of these devices would want to invest in creating two lines of products—one to consort with devices that have something to do with television broadcast content, and one to live in a world unconnected to television. The goal—and the operating assumption—of manufacturers is convergence of the various devices they work with, not separation. Thus, the impact of this rule was designed to be felt across all consumer electronics devices.

This was a direct attack on the openness of these many devices. It was an attack on their ability to connect to other devices and the Internet, to permit transformation and combination of digital content, and to allow for the voluntary creation of information flow membranes. To the extent that any manufacturer of any device wished to have that device connect to devices that touched broadcast content, that manufacturer would have had to comply with the licensing rules authorized by the flag proceeding—which in turn would have limited interoperability to those devices that were themselves compliant.[74] This meant that the device would have had to ensure that its digital outputs were constrained by an Authorized Digital Output Protection Technology. It could not have stored or recorded this content unless access by a noncompliant device to that content could not occur.[75] And once a device was trained to recognize and adhere to the demands of the broadcast flag, there was no reason that many more varieties of digital content would not have been similarly flagged.[76] Open devices that allowed information flows in and out, permitted snippets of content to be mixed with other information and made into a transformative work, and allowed unauthorized access to the results of these transformations were on the way to being forbidden.

The broadcast flag scheme adopted by the FCC (one that Congress may authorize in the wake of the May 2005 D.C. Circuit ruling striking it down) may have been just a first step towards a much more constrained future world of devices.[77] It is a step that will be echoed across the world. Canada will likely move quickly to create a broadcast flag regime.[78]

74. 47 C.F.R. § 73.9004 (2005).

75. *Id.*

76. Broadcasters may choose to use their new spectrum for multi-casting several lower-resolution streams at once—making new digital services possible. There is no limit on the nature of the material to which flags can be applied by broadcasters; wide swathes of data in the public domain could be flagged just as easily as first-run movies.

77. Some might say that the real question is "what can be flagged," rather than "can flagged content traverse the Internet." Because flagging is so easy and subject to no constraints, it will be widely adopted—and may cover public domain content, factual material unprotected by copyright, and news. It is not politically feasible or practically possible to put the genie back in the bottle and mandate limits on what can be flagged.

78. *See* Michael Geist, *Advancing Technology Threatens Cultural Policy*, Toronto Star, Nov. 8, 2004, at D3; Michael Geist, *Mr. Minister, Please Protect the Public Interest*, Toronto Star, Sept. 6, 2004, at C2; Radio Advisory Board of Canada, Key Industry Canada Activities and Priorities for 2005 (2004), http://www.rabc.ottawa.on.ca/e/Files/5.%20IC%20Rpt.doc (stating that standards priority work for 2005 will include "recognition of the broadcast flag").

Moreover, member states of the World Intellectual Property Organization ("WIPO")[79] are continuing work on a treaty[80] that is planned to protect broadcasting signals and webcasts.[81] The current draft of this treaty, which is being pushed hard by the MPAA through U.S. officials, states that the member states "recogniz[e] the need to introduce new international rules in order to provide adequate solutions to the questions raised by economic, social, cultural and technological developments"[82] and grants to broadcasters (and potentially webcasters) for a term of fifty years "the exclusive right of authorizing the retransmission [defined very broadly to include all forms of communication of a broadcast by anyone, including over computer networks] by any means of their broadcasts."[83]

Thus, this treaty would give broadcasters, cablecasters, and, under the U.S. proposal, webcasters, a broad range of new exclusive rights. Although the most recent WIPO discussion of this treaty ended in confusion when the chairman of the responsible committee (in a transparent effort to push the treaty along and isolate dissenters) suddenly called for a vote rather than continuing to work for consensus,[84] it is likely that worldwide protections for broadcasters, webcasters, and the "technical protection measures" they use will be agreed to in some form. It is my view that this treaty is likely to form the basis for global adoption of broadcast flag schemes modeled on the U.S. version.

C. *IP-Enabled Services Background*

On March 10, 2004, the FCC released a Notice of Proposed Rulemaking for IP-enabled services.[85] The FCC made clear that "the scope of this proceeding—and the term 'IP-enabled services,' as it is used here—includes services and applications relying on the Internet Protocol family."[86] Thus, the IP-Enabled Services Notice of Proposed Rulemaking suggests that the Commission views its regulatory authority as extending to end-user software, network hardware, corporate and community websites and more.

---

79. "WIPO is an intergovernmental organization based in Geneva, Switzerland responsible for the promotion of the protection of intellectual rights throughout the world. It is one of the 16 specialized agencies of the United Nations system of organizations." ICANN Glossary, http://www.icann.org/general/glossary.htm (last visited Oct. 20, 2005).

80. WIPO, Member States, http://www.wipo.int/directory/en/member_states.jsp (last visited Oct. 19, 2005).

81. World Intellectual Property Organization, Standing Committee on Copyright and Related Rights, Twelfth Session, *Revised Consolidated Text for a Treaty on the Protection of Broadcasting Organizations*, SCCR/12/2 (Oct. 4, 2004), *available at* http://www.wipo.int/edocs/mdocs/copyright/en/sccr_12/sccr_12_2.doc.

82. *Id.* at 13.

83. *Id.* at 39.

84. Carolyn Deere, *WIPO Broadcasting Treaty Discussions End in Controversy, Confusion*, Intell. Prop. Watch, Nov. 22, 2004, http://www.ip-watch.org/weblog/index.php?p=10&res=1024_ff&print=0.

85. IP-Enabled Servs., 19 F.C.C.R. 4863 (2004) (FCC notice of proposed rulemaking).

86. *Id.* at 4864 n.1.

In the IP Notice of Proposed Rulemaking, the Commission, while acknowledging that the Internet had "become one of the greatest drivers of consumer choice and benefit, technical innovation, and economic development in the United States in the last ten years,"[87] stated that "provisions designed to ensure disability access, consumer protection, emergency 911 service, law enforcement access for authorized wiretapping purposes, consumer privacy, and others [social policy concerns]—should continue to have relevance as communications migrate to IP-enabled services."[88] The IP Notice of Proposed Rulemaking suggests that traditional "common carrier" regulation, in which service providers file tariffs, respond to interconnection obligations, and pay access fees, may not be appropriate for IP-enabled services.[89] But the IP Notice of Proposed Rulemaking indicates that "social policies" may be appropriate for some or all IP-enabled services.[90]

On August 9, 2004, the FCC released its Communications Assistance for Law Enforcement ("CALEA") Notice of Proposed Rulemaking,[91] suggesting that some subset of IP-enabled services should be designed so as to assist law enforcement officials in implementing wiretap orders. The IP Notice of Proposed Rulemaking and CALEA Notice of Proposed Rulemaking are closely linked, and together suggest that online services are subject to "social policy" rules established by the FCC—including the policy that some services be required to build in basic wiretap capabilities.

One key reason for the release of the IP and CALEA Notices was the desire of incumbent telephone companies to maintain a level regulatory playing field in the Internet era. Calls made with VoIP services that connect to the traditional telephone network (the "PSTN") are twenty percent to thirty percent less expensive than calls made using the PSTN, because the Internet is not taxed the way the PSTN is. And calls made with VoIP that do not connect to the PSTN are often completely free or very low cost.[92] This causes heartaches for companies that base their business model on the PSTN, because they are stuck with providing universal telephone service, 911 emergency services, guaranteeing wiretapping access for police, and providing access for the hearing-impaired—and are subject to extensive taxes and fees imposed by the FCC and the states. The rise of

87. *Id.* at 4864.

88. *Id.* at 4867.

89. *Id.*

90. *Id.* The *IP-Enabled Services* Notice of Proposed Rulemaking focuses on questions relating to emergency services, access by individuals with disabilities, consumer protection, and universal service. The FCC uses the term "social policy concerns" as shorthand for this list of issues plus the issues raised in the Communications Assistance for Law Enforcement Notice of Proposed Rulemaking. *See IP-Enabled Servs.*, 19 F.C.C.R. at 4879-80.

91. Commc'ns Assistance for Law Enforcement Act & Broadband Access & Servs., 19 F.C.C.R. 15,676 (2004) (FCC notice of proposed rulemaking and declaratory ruling).

92. Voice of IP ("VoIP") is an IP-enabled service—transmitting telephone calls over a data network, using packet-switching to save costs. *See* NOVACON: Glossary of Internet Terms, Chicago Comparison, VoIP, http://www.novacon.com/faq_s-z.htm (last visited Oct. 20, 2005).

VoIP also causes heartaches for state and federal government. As more people begin using unregulated VoIP applications instead of the taxed traditional telephone system, federal and state governments will start to lose billions of dollars.

By the third quarter of 2003, at least fifteen states either had begun to regulate or were considering the regulation of IP voice offerings.[93] In particular, in September 2003, the California State Public Utilities Commission ("PUC") told six VoIP companies that connect to the PSTN to get a license in order to provide phone services to people in California.[94] Minnesota and New York went the other direction, ruling that VoIP providers—even those connecting to the PSTN—were not subject to state taxing and tariffing.[95] Both the California and New York PUCs announced that they would pull back, giving the FCC time to come up with rules for VoIP. The March 2004 Notice of Proposed Rulemaking was at least in part a response to these state efforts. Vonage, a VoIP company that connects to the PSTN, had successfully called for FCC preemption of any state taxes or regulation of VoIP.[96]

A second reason for the breadth of the IP and CALEA Notices of Proposed Rulemaking was FCC's desire to maintain its relevance in an era of decreasing reliance on telephones.[97] The old world of circuit-switched networks and monopoly providers, on which FCC's regulatory scheme depended, is rapidly being replaced by a new age of packet-switched networks for which scarcity simply is not an issue.[98] To date, and with very

93. *See* Comments of SBC Communications, Inc. at 5-6, Vonage Holding Corp.'s Petition for Declaratory Ruling, WC Docket No. 03-211 (Oct. 27, 2003), *available at* http://www.neca.org/wawatch/wwpdf/102803_36.pdf.

94. The Director of the California Public Utilities Commission, John Leutza, noted that the distinction between land and Internet phone providers was minimal. Ben Charny, *California to Regulate VoIP Providers*, CNET News.com, Sept. 30, 2003, http://news.com.com/California+to+regulate+VoIP+providers/2100-7352_3-5084711.html.

95. The Minnesota Public Utilities Commission ("PUC") ruled that Vonage's VoIP service was an intrastate telephone service, subject to state law. Vonage Holdings Corp.'s Petition for a Declaratory Ruling Concerning an Order of the Minnesota Pub. Util. Comm'n, 19 F.C.C.R. 22,404 (2004) (memorandum opinion and order); *see also* Vonage Holdings Corp. v. Minn. Public Utilities Commission, 290 F. Supp. 2d 993 (D. Minn. 2003). Vonage was able to have the Public Utilities Commission's determination overturned on appeal when a federal judge held that VoIP is an information service not subject to state jurisdiction. Linda Haugsted, *States Wrestle with VoIP Approaches; As Cable Ops and Others Jump into New Phone Frontier, Regulators Eye Turf Defenses*, Vonage Press Room, Jan. 5, 2004, http://www.vonage.com/corporate/press_news.php?PR=2004_01_05_1.

96. *Vonage Petition for a Declaratory Ruling*, 19 F.C.C.R. at 22,404.

97. This is similar to the Interstate Commerce Commission's effort to retain its relevance as the national transportation landscape evolved. *See* Paul Dempsey, *The Insterstate Commerce Commission—Disintegration of an American Legal Institution*, 34 Am. U. L. Rev. 1 (1984-85).

98. Mark A. Lemley & Lawrence Lessig, *The End of End-to-End: Preserving the Architecture of the Internet in the Broadband Era*, 48 UCLA L. Rev. 925 (2001); Jonathan Weinberg, *The Internet and "Telecommunications Services," Universal Service Mechanisms, Access Charges, and Other Flotsam of the Regulatory System*, 16 Yale J. on Reg. 211, 225-38 (1999) ("Packet-switched networks are taking over, and the

modest exceptions that can be directly tied to the FCC's telecommunications authority, the FCC has not had much to say about "regulating the Internet."[99]

Over the last thirty years, the FCC has, however, had something to say about regulating computers—and it has decided to leave them alone. Beginning in 1971, the FCC conducted three proceedings (called Computer I, Computer II, and Computer III) about the relationships between computer data processing (computers used to direct network operations) and telecommunications (end users using computers to communicate) which resulted in FCC pronouncements that where data was transformed by computers in use by common carriers before being presented to human end users, these services (called "enhanced services") would be "unregulated" by the FCC.[100] Basic services, by contrast, which provided only transmission of communications, would be regulated under FCC's "common carrier" Title II regime.[101] The Commission predicted, correctly, that the development and availability of "enhanced services" would best be promoted if regulatory rules and procedures were not "interjected between technology and its marketplace applications."[102]

The passage of the Telecommunications Act of 1996 (the "Act") represented a codification of this "unregulation" approach. The Act defined "Information Services" as "the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications, and includes electronic publishing."[103] The Commission stated that "information services consist of all services that the Commission previously considered to be enhanced

---

communications world is changing."); *see also* Reno v. ACLU, 521 U.S. 844, 868-70 (1997).

99. The FCC did impose conditions in connection with approving the AOL/Time Warner merger, requiring that AOL's instant messaging client interoperate with competitors and that Time Warner should make capacity on its cable systems available for Internet access by competitors. But the FCC's power to impose these conditions was founded exclusively on the FCC's approval of transfers of licenses for Time Warner's cable companies, broadcast companies, and telephone interests to the merged entity. *See* Applications for Consent to the Transfer of Control of Licenses & Section 214 Authorizations by Time Warner Inc. & Am. Online, Inc., Transferors, to AOL Time Warner Inc., Transferee, 16 F.C.C.R. 6547 (2001) (FCC opinion and order).

100. Amendment of Section 64.702 of the Comm'n's Rules & Regulations (Second Computer Inquiry), 72 F.C.C.2d 358 (1979) (tentative decision and further notice of inquiry and rulemaking), *rule modification granted by* 77 F.C.C.2d 384 (1980) (final decision), *reconsidered*, 84 F.C.C.2d 50 (1981), *further reconsidered*, 88 F.C.C.2d 512 (1981), *aff'd sub nom.* Computer & Comm'cns Indus. Ass'n. v. FCC, 693 F.2d 198 (D.C. Cir. 1982), *cert. denied sub. nom*, Nat'l Ass'n of Regulatory Util. Comm'rs, 461 U.S. 938 (1983), *aff'd on second further reconsideration*, 56 Rad. Reg. 2d (P & F) 301 (1984) (FCC opinion and order).

101. Common carriers are subject to rate regulation, tariffs, and co-location rules. Wire or Radio Communications Act, 47 U.S.C. §§ 201-229 (2000); *see* Orloff v. FCC, 124 S. Ct. 2907 (2004).

102. *Amendment of Section 64.702 of the Comm'n's Rules & Regulations*, 77 F.C.C.2d at 429.

103. 47 U.S.C. § 153 (2000).

services."[104] This signaled that all "information services"—an apparently broad category of computer-assisted communications—would be "unregulated" by the FCC (as "enhanced services" had been).[105] In particular, as discussed in Part I, the Act mandated as "policy of the United States" that development and use of the Internet be "unfettered by federal or state regulation."[106]

But as the Internet world continued to explode, some of the regional Bell operating companies—heavily regulated by the FCC—supported the FCC's call for "social polices" to be applied to IP-enabled services.[107] Chairman Michael Powell, in a separate statement accompanying the IP-enabled services Notice of Proposed Rulemaking, said "rules designed to ensure law enforcement access, universal service,[108] disability access and emergency

104. Implementation of Sections 255 & 251(a)(2) of the Commc'ns Act of 1934, as Enacted by the Telecomms. Act of 1996, 16 F.C.C.R. 6417, 6450 n.180 (1999) (FCC report, order, and further notice of inquiry).

105. IP-enabled services convert information from one form to another, process, retrieve and store information, and perform many other functions that constitute information services, including facilitating subscriber interaction with stored information (such as customer profiles). They thus are classified as "information services" to which Title II and certain other regulations do not apply. 47 U.S.C. § 153(20) (defining "information service"). By contrast, "telecommunications services," which are subject to Title II regulations, are defined as "the transmission, between or among points specified by the user, of information of the user's choosing, without change in the form or content of the information as sent and received." *Id.* § 153(43), (46) (2000) (defining "telecommunications" and "telecommunications service").

106. *Id.* § 230(b)(2).

107. *See* Comments of the Verizon Telephone Companies at 1, IP-Enabled Servs., WC Docket No. 04-36 (May 28, 2004), *available at* http://www.neca.org/wawatch/wwpdf/060204_86.pdf (arguing that IP-enabled services are not subject to traditional forms of economic regulation, but should be subject to "discrete requirements only when necessary to support specific policy objectives"); Comments of SBC Communications Inc. at 57, Vonage Holding Corp.'s Petition for Declaratory Ruling, WC Docket No. 03-211 (Oct. 27, 2003), *available at* http://www.neca.org/wawatch/wwpdf/102803_36.pdf ("The Commission's assertion of jurisdiction to address the public policy concerns surrounding IP-enabled services would not remotely thwart, and is indeed necessary to promote, the substantive policy goals of the Communications Act."). As BellSouth argued,

> To the extent that a particular IP-enabled service is an "information service" under the law, the Commission should leave such services largely unregulated except to the extent that, under its Title I authority, the Commission needs to establish clear expectations with regard to social obligations such as public safety, universal service, 911 and disability access.

Comments of BellSouth Corporation at 23, IP-Enabled Servs., WC Docket No. 04-36 (May 28, 2004), *available at* http://hraunfoss.fcc.gov/edocs_public/SilverStream/Pages/edocsAdvanceSearch.html; *cf.* Comments of Qwest Communications International Inc. at 36, IP-Enabled Servs., WC Docket No. 04-36 (May 28, 2004), *available at* http://gullfoss2.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=6516199524 (advocating that the Commission should exercise its ancillary jurisdiction to apply noneconomic regulations to IP-enabled services and applications only on a showing of necessity to achieve an important objective under the Telecommunications Act).

108. "Universal service" is a shorthand designation for a very complicated set of implicit and explicit subsidies initiated in the 1930s that attempt to provide phone service to everyone in the U.S. regardless of distance from central switches or ability to pay. FCC, Universal

911 service can and should be preserved in the new architecture."[109] The FCC had found a new role for itself: ensuring "social policy" structures in the online world. This would enable the FCC to remain relevant and necessary in the age of the Internet, while not extending all of the old economic tariffing rules to online services.

There is substantial tension between this stance and the FCC's overall deregulatory (or "unregulatory") agenda. When Pulver.com filed a petition for a declaratory rulemaking with the FCC, asking that its Free World Dialup ("FWD") service (which is essentially an instant messaging service with voice capabilities that does not connect to the traditional telephone system) be declared not to be a "telecommunications service," the FCC responded that FWD was an "unregulated information service subject to FCC's jurisdiction."[110] In other words, the FCC put FWD in the bucket of services that are not subject to tariffs and rate regulation under Title II of the Communications Act.[111] In general, then-Chairman Powell was vocal in his support for an "unregulated" Internet, at one point telling USA Today, "If you're going to say to me that Voice over IP is something that needs regulation, then you're going to have to explain to me why e-mail isn't also, or streaming video or instant messaging is not also."[112]

Some media outlets read this "unregulation" and "nonregulation" language to mean that Internet applications would remain unregulated by the FCC.[113] But "unregulation" does not mean "no regulation." "Social

---

Service Home Page, http://www.fcc.gov/wcb/universal_service/welcome.html (last visited Oct. 20, 2005) (providing the FCC's definition of "universal service").

109. IP-Enabled Servs., 19 F.C.C.R. 4863, 4951 (2004) (notice of proposed rulemaking, separate statement of Commissioner Michael K. Powell); *see also IP-Enabled Servs.*, 19 F.C.C.R. at 4893.

> Congress stated that the Internet should remain free from regulation. But Congress also has stated public policy goals that would presumably continue to apply as communications networks evolve. For example, it has stated that universal service should be maintained, that telecommunications equipment and services should remain usable by people with disabilities, that prompt emergency service should be available to the public through the 911 system, and that communications should be accessible to law enforcement officers acting on the basis of a lawfully obtained warrant.

Id. (footnote omitted). All of these "public policy goals" have been expressed in the past by Congress with respect only to telecommunications services—common carriers.

110. Petition for Declaratory Ruling that pulver.com's Free World Dialup Is Neither Telecomms. Nor a Telecomms. Serv., 19 F.C.C.R. 3307, 3307 (2004).

111. Communications Act of 1934, Pub. L. No. 73-416, 48 Stat. 1064 (codified as amended in scattered sections of 47 U.S.C.).

112. Reuters, *FCC Chief Plans No Internet Phone Regulation*, USA Today, Jan. 22, 2004, at 1B.

113. The headline for the FCC's press release announcing the pulver.com decision read, "FCC Rules that pulver.com's Free World Dialup Service Should Remain Free From Unnecessary Regulation," and many people understood this to mean that IP-enabled services would not be subject to any rules imposed by the FCC. Press Release, Fed. Commc'n Comm'n, FCC Rules That pulver.com's Free World Dialup Service Should Remain Free from Unnecessary Regulation (Feb. 12, 2004), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-243869A1.pdf; *see, e.g.*, Interview with Jeff Pulver, Co-founder, Vonage, BroadBandReports.com (Feb. 18, 2004), http://www.dslreports.com/shownews/39049 ("Your victory, thanks to years of effort, for the

policies," including design mandates under CALEA and payment into Universal Service funds, were envisioned by the FCC to be part of "unregulation." Although it is still quite unclear what social policies the FCC will require of what categories of IP-enabled services, the FCC's stance is consistent: The Commission strongly believes it has the authority to bring social policies to bear on the Internet, and has put forth a menu of such policies that it believes may apply to IP-enabled services.

D. *CALEA Background*[114]

Unlike the flag context, in which we have a fully articulated (if temporarily stalled) regime to look at, most of the IP-enabled services/CALEA "social policies" rulemaking is still wide open for discussion. But the CALEA process signals that the FCC may take the view that permission will be needed from government authorities when designing a wide variety of services, computers, and web sites that use the Internet protocol. In other words, information flow membranes will be governmentally mandated as part of the design process for online products and services.

Under the federal wiretap statute, all electronic communications—no matter whether they are in the form of faxes, emails, or VoIP calls—can be intercepted legally if a wiretap order has been obtained.[115] Any provider of any electronic communications service is required to furnish information and technical assistance for such an interception.[116]

With the rise of digital telephony in the early 1990s, law enforcement was worried that new digital systems would be more difficult to tap than analog systems, and wanted to ensure that it would be able speedily to implement wiretap orders. Law enforcement may also have wanted to shift the cost of adjusting to different telecommunications carriers' systems to the carriers themselves. After substantial narrowing negotiations, CALEA was enacted in 1994.[117] CALEA requires that telecommunications

---

time being frees [Free World Dial-Up] and other 'pure' VoIP providers from regulation. Do you expect further battles down the road?").

114. Some portions of this section appear in revised form in Susan P. Crawford, Someone to Watch over Me: Social Policies for the Internet (2005) (unpublished manuscript, on file with author).

115. Wire and Electronic Communications Interception and Interception of Oral Communications, 18 U.S.C. §§ 2510-2522 (2000). Thus, cable companies, broadband access providers generally, and VoIP service providers are all already subject to a surveillance assistance requirement. *Id.* § 2518(4).

116. *See id.* § 2518(4).

117. Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified as amended at 18 U.S.C. § 2522 and 47 U.S.C. §§ 229, 1001-1010 (2000)). Then-Federal Bureau of Investigation Director Louis Freeh said during a joint congressional hearing on the Communications Assistance for Law Enforcement Act ("CALEA") in 1994 that a broader bill covering all communications service providers had been "rejected out of hand." J. Hearings on H.R. 4922 and S. 2375 Before the Subcomm. on Tech. and the Law of the S. Comm. on the Judiciary and the Subcomm. on Civil and Const'l Rights of the H. Comm. on the Judiciary, 103rd Cong. 49 (1994).

providers—common carriers of telephone communications[118]—provide certain specific capacities and capabilities to make wiretapping easier for law enforcement.

Even though the Internet had not come into common use in 1994, Congress was then well aware of the differences between circuit-switched and packet-switched networks that I have described above.[119] Congress specifically elected to leave Internet services out of CALEA's coverage.[120]

With the increasing popularity of VoIP services, law enforcement became concerned that it would become difficult to wiretap online communications that, from their perspective, were equivalent to traditional telephone calls. In March 2004, the Department of Justice ("DOJ"), the Drug Enforcement Agency ("DEA"), and the Federal Bureau of Investigation ("FBI") filed a joint petition asking the FCC to begin a rulemaking proceeding focused on CALEA implementation for broadband access services and broadband telephony.[121] Shortly thereafter, bills were introduced in both the Senate[122] and House[123] that would have given the FCC express jurisdiction over VoIP, but neither bill had passed either the Senate or the House at the time this Article was prepared.

On August 9, 2004, when the FCC released its CALEA Notice of Proposed Rulemaking, it said,

> [T]he Commission tentatively concludes that CALEA applies to facilities-based providers of any type of broadband Internet access service—including wireline, cable modem, satellite, wireless, and powerline—and to managed or mediated Voice over Internet Protocol ("VoIP") services. These tentative conclusions are based on a Commission proposal that these services fall under CALEA as "a replacement for a substantial portion of the local telephone exchange service."[124]

---

118. 47 U.S.C. § 1001(8)(A).

119. *See supra* note 17.

120. *See* 47 U.S.C. § 1002(b)(2); *see also* U.S. Telecomm. Ass'n v. FCC, 227 F.3d 450, 455 (D.C. Cir. 2000) ("CALEA does not cover 'information services' such as e-mail and Internet access."); H.R. Rep. No. 103-827(I), at 23 (1994) *as reprinted in* 1994 U.S.C.C.A.N. 3489, 3503 (stating that CALEA obligations "do not apply to information services, such as electronic mail services, or on-line services, such as Compuserve, Prodigy, America On-line or Mead Data, or Internet service providers"). The Commission has found that information services "such as electronic mail providers and on-line service providers" are exempt from CALEA. Commc'ns Assistance for Law Enforcement Act, 15 F.C.C.R. 7105, 7119 (1999) (FCC second report & order).

121. Joint Petition for Expedited Rulemaking, U.S. Dep't of Justice, Fed. Bureau of Investigation & Drug Enforcement Admin. Joint Petition for Rulemaking to Resolve Various Outstanding Issues Concerning the Implementation of the Commc'ns Assistance for Law Enforcement Act, RM No. 10865 (FCC Mar. 10, 2004), *available at* http://www.askcalea.net/docs/20040310.calea.jper.pdf.

122. VoIP Regulatory Freedom Act of 2004, S. 2281, 108th Cong.

123. Advanced Internet Communications Services Act of 2004, H. 4757, 108th Cong.

124. Press Release, Fed. Commc'n Comm'n, FCC Adopts Notice of Proposed Rulemaking and Declaratory Ruling Regarding Communications Assistance for Law Enforcement Act (Aug. 4, 2004), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-250547A3.pdf.

Then, on August 5, 2005 the FCC ruled that broadband Internet access and "interconnected VoIP" services must be designed so as to make government wiretapping easier.[125]

The strength of the Commission's arguments for CALEA application to broadband services and VoIP will come under immediate scrutiny, because there is an exemption under section 102(8) of CALEA for "information services," and VoIP is an "information service."[126] In a comment accompanying the August 5, 2005 press release, FCC Commissioner Kathleen Abernathy noted the weakness of the FCC's legal claim, saying,

> Because litigation is as inevitable as death and taxes, and because some might not read the statute to permit the extension of CALEA to the broadband Internet access and VoIP services at issue here, I have stated my concern that an approach like the one we adopt today is not without legal risk.[127]

Thus, in sum, the FCC interpreted the CALEA statute (which focused exclusively on digital technology within the PSTN) to address online information applications—a category of technologies specifically excluded from CALEA's scope. Indeed, filed comments in the CALEA proceeding suggest that law enforcement authorities are interested in having CALEA apply to all online applications.[128]

What VoIP services would be required to do to assist law enforcement remains quite unclear. Under CALEA, telecommunications carriers are required to (1) enable law enforcement, pursuant to a court order or other lawful authorization, to access "call-identifying information" that is "reasonably available" to the carrier, and (2) to deliver access to call-identifying information in a format that may be transmitted to a remote location. It appears that in requesting that CALEA be extended to Internet services, law enforcement will likely demand that standardized information be created in a form acceptable to them. The only limitation proposed in the CALEA Notice of Proposed Rulemaking on this subject is that information will not be considered to be "reasonably" available if the

---

125. Press Release, Fed. Commc'n Comm'n, FCC Requires Certain Broadband and VoIP Providers to Accommodate Wiretaps, Order Stikes Balance Between Law Enforcement, Innovation (Aug. 5, 2005).

126. *See infra* notes 208-11 and accompanying text .

127. Statement of Kathleen Q. Abernathy, FCC Commissioner, *In re* Communications Assistance for Law Enforcement and Broadband Access and Services (Aug. 5, 2005), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-260434A3.pdf.

128. Comments of Eliot Spitzer, Attorney General for the State of New York at 9-10, Commc'ns Assistance for Law Enforcement Act & Broadband Access and Servs., ET Docket No. 04-295 (FCC Nov. 8. 2004), *available at* http://www.oag.state.ny.us/telecommunications/filings/ag_calea.pdf; Comments of the United States Department Of Justice at 32-33, Commc'ns Assistance for Law Enforcement Act & Broadband Access & Services, ET Docket No. 04-295 (FCC Nov. 8, 2004), *available at* http://www.askcalea.com/docs/20041108_doj_comments.pdf [hereinafter DOJ CALEA Comments] (arguing that involvement in any ongoing flow of information among Internet users should be considered "management," and any online services may be included in this category—not just those that interconnect with the traditional telephone network).

information is only accessible by "significantly modifying a network."[129] This is very little protection for Internet services, and it seems likely that such services will end up implementing data and functionality designs that are pleasing to law enforcement. More importantly, "call identifying information" is specifically not supposed to be available under CALEA where such information "may disclose the physical location of the subscriber" in the absence of a lawful court order (more than just a pen register or trap and trace order).[130] Online, of course, all Internet communications "may disclose" this information—IP addresses can sometimes perform this function, and the Session Initiation Protocol used for many VoIP calls will convey the physical location of the end user.[131]

So far, law enforcement has refused to say what it means by "call identifying information" for the Internet,[132] and has suggested that such information may be different for different entities.[133] Law enforcement would like the discretion to negotiate with technology companies over what is meant by "call identifying information" and in what form it must be sent to them.[134] Just as innovators in content protection technologies were beaten down by the MPAA when they wanted to allow encrypted content to traverse the public Internet in the flag proceedings, here the FBI will preapprove the design and capabilities of Internet services—with a great deal of enforcement power behind it. Law enforcement wants to decide, once a general rule is in place, what products or services are covered by CALEA, what information is required to be furnished to them and in what form, and who should pay for what.

Most critically for the future of the Internet, law enforcement in the CALEA proceeding has made clear that it wants to ensure that it reviews all possibly relevant new services for compliance with unstated information-gathering and information-forwarding requirements before these services are launched. All prudent businesses will want to run their services by law enforcement, suggests the DOJ: "Service providers would be well advised to seek guidance early, preferably well before deployment of a service, if they believe that their service is not covered by CALEA. . . . DOJ would

129. Commc'ns Assistance for Law Enforcement Act & Broadband Access & Servs., 19 F.C.C.R. 15,676, 15,714 (2004) (FCC notice of proposed rulemaking and declaratory ruling).

130. 47 U.S.C. § 1002(a)(2) (2000).

131. The Internet Engineering Task Force ("IETF") is working on exactly this issue. *See* James M. Polk & Brian Rosen, Internet Engineering Task Force, Internet Draft, Requirements for Session Initiation Protocol Conveyance (Oct. 25, 2004), http://tools.ietf.org/wg/sipping/draft-ietf-sipping-location-requirements/draft-ietf-sipping-location-requirements-02.txt.

132. DOJ CALEA Comments, *supra* note 128, at 42.

133. *Id.* at 7.

134. The Department of Justice ("DOJ") has stated that it prefers to use a secondary, negotiating process under CALEA that can only take place after a particular service has entered the marketplace and been found wanting by law enforcement (the "deficiency process") to discuss the meaning of "call identifying information." *Id.* at 42.

certainly consider a service provider's failure to request such guidance in any enforcement action."[135]

This is a threat: Come negotiate with us first, or you will run the risk of being subject to penalties later. And, of course, innovators will not know to what standards they are being held during these negotiations—what "call identifying information" means on the Internet, what form service providers will have to provide it in, or what capabilities they will have to provide law enforcement. Most alarmingly of all, these negotiations will inevitably end up in design mandates; according to the DOJ, "any definition of 'reasonably available' [call identifying information] should be based on the technical solutions a carrier and vendor can achieve when they first design the network, not on the unfortunate realities that prevail after a non-compliant network has already been constructed."[136]

E. *IP-Enabled Services and Membranes*

The threats to collective creation of information-flow membranes posed by the IP-enabled/CALEA rulemakings are clear. The DOJ will seek to penalize service providers that do not submit their applications for pre-launch CALEA review. Law enforcement will want to bring "deficiency" proceedings against any online service or application provider that they deem to be covered by CALEA.

What does this foretaste of the FCC's likely actions on CALEA signal for the open Internet? The central presumption of Internet innovation will likely be flipped as a result of this proceeding: Instead of "everything not prohibited is permitted," the new default setting will be "everything not permitted is prohibited." All new online services will eventually be subject to law enforcement "compliance" review before they go on the market. There is no limiting principle for law enforcement's interpretation of its need: Because a voice bit is indistinguishable from a data bit, all services will eventually be covered by the DOJ's interpretation of CALEA. And we will not know until later what law enforcement's design mandates will be, because all of this will be negotiated behind closed doors. All prudent businesses seeking to avoid deficiency findings will feel the need to go ask permission before launching. So CALEA will be a high and expensive barrier to innovation. Smaller outfits will simply crumble rather than go through pre-launch law enforcement review, collaborative and open-source innovations will not pass law enforcement's tests, and a pall of uncertainty will be cast over the entire scene. In sum, the FCC through this expansion of CALEA will create mandatory membranes for applications that are used online.

---

135. *Id.* at 36 n.123, 38.

136. *Id.* In many other places in its filing, DOJ makes clear that it is seeking prelaunch review of services that it might interpret are subject to CALEA obligations. For example, according to DOJ, "CALEA's purpose [is] to ensure solutions are built in pre-deployment." *Id.* at 21.

As with the push for the broadcast flag, the push for extension of CALEA to the Internet (and for delegation of broad design discretion to law enforcement) is being echoed worldwide. The Council of Europe's Convention on Cybercrime (signed by the United States but not yet ratified)[137] broadly requires service providers to provide assistance to law enforcement for lawful interception of all electronic communications.[138] Each ratifier of the Convention is required to "empower its competent authorities" to "compel" service providers, "within [their] existing technical capability," to cooperate and assist the competent authorities in the interception and recording of both "traffic data"[139] and "content data" in real time of communications transmitted by means of a computer system.[140] And service providers are to be obliged to "keep confidential the fact of and any information about the execution of any power provided for" in these surveillance provisions.[141] These are broader requirements than any

137. The terms of the Convention required that it would enter into force only once it had been ratified by five countries, at least three of which were Member States of the Council of Europe. In July 2004 the Convention entered into force, having been ratified by Albania, Croatia, Estonia, Hungary, Lithuania, and Romania. Sen. Lugar's Foreign Relations Committee held a mostly favorable hearing on the Convention in June 2004. It is likely that the U.S. will ratify the Convention in 2005. An optional additional protocol on hate speech will likely not be ratified by the U.S., and indeed has not yet (as of September 2005) been ratified by any countries. *See* Convention on Cybercrime, Nov. 23, 2001, 41 I.L.M. 282, *available at* http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm; Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems, Jan. 28, 2003, *available at* http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm.

138. For text of the treaty, see Convention on Cybercrime, *supra* note 137. Intellectual property and surveillance concerns often converge; article 10.1 of the Convention includes vague language suggesting that infringement using a computer system should be criminalized: "Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright . . . where such acts are committed willfully, on a commercial scale and by means of a computer system." *Id.* art. 10, § 1.

139. "'[T]raffic data' means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service." *Id.* art. 1(d). "Content data" is not defined in the Convention. VeriSign, in its comments to the FCC in connection with the CALEA proceeding, takes the position that the CALEA term "call identifying information" for Internet communications should be taken to mean "traffic data" as defined in the Convention, and that

> [a]ll object-to-object communication should constitute realtime traffic data, not content. Only humans generate "content." Because the privacy protections accorded to human communications "content" impose such substantial overheads, complexities, and costs on both providers and law enforcement to implement those protections, the definition of "content" in the context of CALEA should be narrowly construed.

Comments of VeriSign, Inc. at 18, Commc'ns Assistance for Law Enforcement Act & Broadband Access & Servs., ET No. 04-295 (FCC Nov. 8, 2004) [hereinafter VeriSign Comments], *available at* https://67.15.34.213/dmirror/http/www.cdt.org/digi_tele/20041108verisign.pdf.

140. *See* Convention on Cybercrime, *supra* note 137, arts. 20, 21.

141. *Id.* art. 21, § 3.

possible reading of CALEA would support, as CALEA specifically deals with non-content data and does not gag service providers.[142]

Through the domestic CALEA/IP-enabled services proceeding and the Council of Europe's Convention on Cybercrime, governments are working towards control of an unlimited array of Internet services in the name of preventing crime. The U.N.'s International Telecommunication Union ("ITU") has blandly predicted that such controls are inevitable for the Internet:

> [A]s the Internet transitions to a [Next Generation Network ("NGN")] infrastructure, on which critical public services are layered, dependent on differing national policy, legislative and regulatory environments, there will also [be] a consideration of similar or identical rules applied to services offered over current circuit-switched networks. Such examples might include provisions for public safety needs, disability assistance, *law enforcement support (in particular, legal interception)*, competition considerations, fraud prevention, prioritization during emergencies, privacy and data protection, and consumer protection against unwanted intrusions. These requirements in turn assist in identification of areas likely to require international standardization activity.[143]

The harmonization between the U.N.'s language and that of the FCC in its IP-enabled services Notice of Proposed Rulemaking is unmistakable. We are in for a drawn-out global battle between the forces of centralization and decentralization, between rigidity and openness.

The FCC rulemakings assessed in this Article are important milestones along our path: They involve incremental technical mandates and pre-approval processes affecting the Internet that both reserve in the FCC the power to do much more and are being echoed around the world. In particular, the U.N. created a Working Group on Internet Governance ("WGIG") that issued a broad report in June 2005.[144] The WGIG considered "whether there will be international regulation of such things as spam, fraud and content that's considered inappropriate."[145] The WGIG adopted an extraordinarily broad Plan of Action, a document more than 20

142. Indeed, the Convention provisions dealing with interception of content data was kept secret until just before the deadline provided by the Council of Europe for comments. *See generally* Yaman Akdeniz, Cyber-Rights & Cyber-Liberties: An Advocacy Handbook for the Non-Governmental Organizations (2003), http://www.cyber-rights.org/cybercrime/coe_handbook_crcl.pdf.

143. U.N. Int'l Telecomm. Union, Council Working Group on the World Summit on the Information Society, *Beyond Internet Governance*, at 11, U.N. Doc WG-WSIS 7/13-E (Dec. 8, 2004), *available at* http://www.itu.int/council/wsis/Geneva3_04/intgov-contribution-wg-wsis.doc. Indeed, in VeriSign's view, "[t]he implementation of real-time traffic data and content production requirements under the Cybercrime Convention and numerous MLATs effected for law enforcement, critically depends on global standards solutions for Next Generation Networks, including IP-Enabled services and VoIP." Verisign Comments, *supra* note 139, at 24.

144. Report of the Working Group on Internet Governance (June 2005), http://www.wgig.org/docs/WGIGREPORT.pdf.

145. *WSIS Participants Struggle to Reach Internet Governance Consensus*, Washington Internet Daily, July 26, 2004, http://www.warren-news.com/internetservices.htm.

pages long, addressing issues ranging from connectivity for small rural villages to joint prosecutions of cybercrime, from "appropriate action on spam" to e-health initiatives.

There is a deep agenda underneath the WGIG efforts: a quest to "govern" the Internet just like telecommunications lines, by making it subject to imposed membranes. As Markus Kummer, secretariat of the WGIG, makes clear, "[t]here are some member states within the U.N. that would like to think the Internet itself is a communications medium that should be regulated like the telecom industry."[146] And there are deep ties between the U.N.'s ITU, which is staffing the WGIG and would like to take over some of the Internet Corporation for Assigned Names and Number's ("ICANN") functions,[147] and local telecom agencies, which would like to have control over new turf involving Internet-specific regulations.[148] Common cause has been easy to find within these groups. These local telecom agencies, which are used to dealing with communications media in a governmental way, may be looking to harmonize "social policy standards" for content worldwide.[149] "Social policies" may themselves signal the end of decentralized creation of membranes, by prompting the use of routers to discriminate against particular kinds of content (packets containing VoIP or unauthorized video), or requiring ISPs not to connect to networks deemed to be places where unauthorized content is routinely available, or requiring law enforcement pre-approval for new Internet services.

Part IV makes clear that the FCC's jurisdictional determinations should not be deferred to as a matter of law. But the telecommunications, content, and law enforcement "industries" are not going to give up on constraining the information flows of the Internet, the applications that run over it, and the devices that attach to it. Reversals by courts will lead only towards action on Capitol Hill, and it is there that the battle will be joined.

IV. DOMESTIC LEGAL ANSWERS

If it is true (a) that recent actions of the FCC threaten the openness of the Internet and the voluntariness of the information flow membranes that can be created online, and (b) that these actions are being echoed in different ways around the world, what should be done about this state of affairs?

146. Interview with Markus Kummer, Head Secretariat of the United Nations Working Group on Internet Governance, International Telecommunication Union, http://www.circleid.com/posts/interview_with_united_nations_head_secretariat_of_wgig/ (last visited Oct. 23, 2005).

147. *ITU Chiefs Target ICANN Turf*, Computer Bus. Rev. Online, Dec. 20, 2004, http://www.cbronline.com/article_news.asp?guid=7BB966AD-2017-4673-A034-AA0083A2E492 (stating that the International Telecommunication Union ("ITU") "has been working, mostly quietly, to get its hands on ICANN's responsibilities over the domain name system and IP address allocation for a number of years").

148. ITU's members are telecommunications companies and nations. *See* International Telecommunication Union, Overview, http://www.itu.int/GlobalDirectory/index.html (last visited Oct. 22, 2005).

149. *See* Johnson et al., *supra* note 59.

This part examines possible domestic legal responses to the broadcast flag scheme and the IP-enabled services/CALEA proceedings. Both the broadcast flag and IP-enabled services are being based on the FCC's "ancillary jurisdiction" under Title I of the Communications Act.[150] As this part will demonstrate, the FCC's arguments in these two rulemakings in support of its exercise of jurisdiction are weak, and its determinations on this score should not be deferred to under the *Chevron* doctrine. Similarly, the Commission's statutory argument for extension of CALEA to the Internet is fatally flawed. All of this points towards referral to Congress of the policies and rules suggested in these rulemakings.

A. *The Communications Act and Ancillary Jurisdiction*

The FCC has stated that it is basing its actions in the broadcast flag and IP-enabled services rulemakings on its "ancillary" jurisdiction under Title I of the Communications Act. This section rebuts this argument.

The general purpose of the Communications Act of 1934 (amended in 1996) is to "make available . . . to all the people of the United States, a rapid, efficient, nationwide, and worldwide wire and communication service with adequate facilities at reasonable charges."[151] The Act grants regulatory authority to the FCC over three specific modes of communication services: (a) interstate common carriers under Title II, (b) spectrum licensees under Title III, and (c) cable operators under Title VI.[152] Because manufacturers of consumer electronics equipment and providers of IP-enabled services are neither Title II common carriers, Title III spectrum licensees, nor Title VI cable operators, the FCC looks back to Title I of the Act—where it believes its interstitial or general-purpose authority is found—to support its jurisdiction over these entities.

Title I is quite general. It creates the FCC "[f]or the purpose of regulating interstate and foreign commerce in communication by wire and radio," in order to "make available, so far as possible, to all the people of the United States, without discrimination on the basis of race, color, religion, national origin, or sex, a rapid, efficient, Nationwide, and world-wide wire and radio communication service with adequate facilities at reasonable charges."[153]

Section 2(a) of Title I states that

> [t]he provisions of this act shall apply to all interstate and foreign communication by wire or radio and all interstate and foreign transmission of energy by radio, which originates and/or is received within the United States, and to all persons engaged within the United States in such communication or such transmission of energy by radio.[154]

150. 47 U.S.C. §§ 151-161 (2000).
151. *Id.* § 151.
152. *Id.* §§ 201-276, 301-399(b), 401-416.
153. *Id.* § 151.
154. *Id.* § 152(a).

This section is about scope of coverage—it intentionally excludes people in the Canal Zone, for example—and says nothing about rulemaking authority.[155]

Section 4 of Title I is a lengthy housekeeping section that defines the membership of the FCC, sets forth rules about reimbursement of travel expenses, makes policies about the number of assistants each Commissioner may hire, and sets rates for overtime pay of field engineers.[156] Deeply buried after all of this text, the Act states in 4(i) that "[t]he Commission may perform any and all acts, make such rules and regulations, and issue such orders, not inconsistent with this chapter, as may be necessary in the execution of its functions."[157] This "necessary and proper" section seems to be wholly focused on internal housekeeping, allowing the Commission to make rules that permit it to operate smoothly.[158] Indeed, this crucial section 4(i) arguably allows the Commission only to implement regulations that are necessary to carry out its explicit responsibilities under the Communications Act, and conveys no independent, stand-alone basis for legislative rulemaking authority to the Commission.[159] Most importantly, section 4(i) is not tied to any provisions for sanctions. Reading 4(i) to do more than permit internal housekeeping would render the rulemaking provisions found in Titles II, III, and VI superfluous.[160]

---

155. *See* Thomas G. Krattenmaker & A. Richard Metzger, Jr., *FCC Regulatory Authority over Commercial Television Networks: The Role of Ancillary Jurisdiction*, 77 Nw. U. L. Rev. 403, 404 (1982).

> [I]t is unclear how the Commission may regulate [television] network behavior even under this expansive provision of the Act [section 2(a)], unless the provision is construed to give the FCC authority over everyone in the United States who uses wire or radio electronic communications facilities, such as by talking on the telephone.

Id. at 405.

156. 47 U.S.C. § 154.

157. *Id.* § 154(i).

158. *See* N. Am. Telecomm. Ass'n v. FCC, 772 F.2d 1282, 1292 (7th Cir. 1985) (holding that § 154(i) authorizes the FCC to adopt rules "to the extent necessary to regulate effectively those matters already within the boundaries" of the Act); AT&T v. FCC, 487 F.2d 865, 872 (2d Cir. 1973) (stating that "Congress, rather than purporting 'to transfer its legislative power to the unbounded discretion of the regulatory body,' . . . intended a specific statutory basis for the Commission's authority" (quoting FCC v. RCA Commc'ns, Inc., 346 U.S. 86, 90 (1953))).

159. Motion Picture Ass'n of Am. v. FCC, 309 F.3d 796, 806 (D.C. Cir. 2002); New England Power v. Fed. Power Comm'n, 467 F.2d 425, 430-31 (D.C. Cir. 1972) ("Necessary and proper" rulemaking provisions "merely augment existing powers conferred on the agency by Congress, they do not confer independent authority to [regulate]."), *aff'd*, 415 U.S. 345 (1974).

160. Thomas Merrill and Kathryn Watts have made this argument persuasively. Thomas W. Merrill & Kathryn Tongue Watts, *Agency Rules with the Force of Law: The Original Convention*, 116 Harv. L. Rev. 467, 517-19 (2002) (stating that rulemaking grants not coupled with any provision for sanctions should be understood to authorize only interpretive and procedural rules.) James Speta agrees with this interpretation. James B. Speta, *FCC Authority to Regulate the Internet: Creating It & Limiting It*, 35 Loy. U. Chi. L.J. 15 (2003). However, Philip Weiser advocates for a broader, "common-law" use of Title I ancillary authority to reach Internet-related services:

In the context of both the flag rule and the IP-enabled services proceeding, the FCC has pointed to the language of section 4(i) as giving it broad "ancillary" rulemaking jurisdiction to adopt the relevant rule. Indeed, the FCC asserts that unless Congress has told the Commission it cannot regulate, it has the power to adopt any rules that "effectuate the goals" of the Communications Act.[161]

It is true that Supreme Court decisions of more than thirty years ago interpreted the Communications Act to grant the Commission the authority to regulate cable television based on the idea that such regulation was "reasonably ancillary" to the Commission's statutory authority over broadcast television.[162] The Commission clearly had the power to issue legislative rules that regulated the activities of broadcasters. But when the FCC then asserted legislative rulemaking authority over the operators of cable systems, it had not been delegated by Congress any power to regulate these actors. The Supreme Court's decisions to authorize the Commission to proceed with rules affecting cable operators have been labeled by Thomas Merrill as "spectacular breaches of principle" and as examples of an agency using legislative powers outside the area of its delegated jurisdiction.[163] The Commission is now leaning heavily on these decisions, and on this secondary type of regulatory rulemaking jurisdiction, which is not based on any of the explicit rulemaking authorities granted in Titles II, III, or VI.[164]

The 1968 case that made ancillary jurisdiction famous is *United States v. Southwestern Cable*.[165] The case began when Midwest Television alleged that Southwestern Cable Company was cablecasting Los Angeles stations into the San Diego area, which was hurting the local San Diego broadcast station. The FCC had initially found that cable systems were neither common carriers nor broadcasters, and so FCC had no primary jurisdiction over them. The Commission sought Congressional approval of its jurisdiction over cable, but to no avail. The Commission then went ahead with making rules for the cable industry, and ordered Southwestern not to

---

> Rather than mapping and adjusting the scope of current policies onto the Internet, the development of a new regime pursuant to Title I can ensure that the Internet will prosper and compete with existing media without being encumbered by legacy regulations that may not be appropriate.

Philip J. Weiser, *Toward a Next Generation Regulatory Strategy*, 35 Loy. U. Chi. L.J. 41, 61 (2003).

161. Brief for Respondents, *supra* note 71, at 23, 25; Digital Broad. Content Prot., 18 F.C.C.R. 23,550, 23,563 (2003) (FCC report, order, and further notice of proposed rulemaking).

162. United States v. Midwest Video Corp., 406 U.S. 649, 657-58 (1972); United States v. Sw. Cable Co., 392 U.S. 157, 178 (1968).

163. Merrill, *supra* note 8, at 2169-70.

164. Congress later changed the Communications Act to provide for FCC regulation of cable systems. Cable Communications Policy Act of 1984, 47 U.S.C. § 521 (2000).

165. 392 U.S. at 178.

expand into areas where it had not been cablecasting before February 1966.[166]

When Southwestern Cable appealed to the Ninth Circuit, that court held that the FCC lacked jurisdiction to issue such an order.[167] The Supreme Court granted certiorari on the question of the Commission's authority to promulgate rules prohibiting importation of "distant signals" into the San Diego television market.[168] The *Southwestern Cable* Court found that the FCC's assertion of jurisdiction was appropriate, holding that cable television was an instrument of "'interstate and foreign communication by wire or radio'" within the meaning of section 2(a) of the Communications Act of 1934.[169] For this reason the Commission was held to have "regulatory authority" over cable television.[170] However, the Court chose not "to determine in detail the limits of the Commission's authority to regulate [cable television]" under section 2(a).[171] Instead, stressing that "'the achievement of an agency's ultimate purposes'" was at stake,[172] the Court noted that the rules were "reasonably ancillary to the effective performance of the Commission's various responsibilities for the regulation of television broadcasting."[173] Thus, even though no express statute had been passed supporting FCC's power over cable television, the Court reasoned that because Title III gave the Commission authority to ensure exclusive broadcasting areas or zones, the general "wire or radio" statute provided statutory authority to which the cable authority was "reasonably ancillary."[174]

Following *Southwestern Cable*, the Court expanded the broad outlines of "ancillary jursdiction" that had been created in that case. In *United States v.*

166. The purpose of these rules was to prevent division of audiences and revenues between cable television and fledgling ultra high frequency ("UHF") and educational television stations. Competition by cable operators, the Commission feared, would make these new ventures unprofitable, thereby frustrating the Commission's long-standing and congressionally approved policy of attempting to provide locally controlled broadcast television service. *See id.* at 175 & nn.41-42.

167. Sw. Cable Co. v. United States, 378 F.2d 118 (9th Cir. 1967), *rev'd*, 392 U.S. 157 (1968).

168. *Sw. Cable Co.*, 392 U.S. at 159-60.

169. *Id.* at 167-69 (quoting 47 U.S.C. § 152(a)).

170. *Id.* at 173.

171. *Id.* at 178.

172. *Id.* at 177 (quoting Permian Basin Area Rate Cases, 390 U.S. 747, 780 (1968)).

173. *Id.* at 178.

174. *Id.* at 175, 178. In 1976, in *National Association of Regulatory Utility Commissioners v. FCC*, the D.C. Circuit interpreted *Southwestern Cable* to be based on the Commission's power to require such zone exclusivity:

> The Supreme Court's decision [in *Southwestern Cable*] to define F.C.C. jurisdiction over cable operators in terms of its jurisdiction over television broadcasting emanated from a finding that the two operations would otherwise conflict rather than from a determination that cable television fit neatly within the Communications Act provisions governing broadcasters.

533 F.2d 601, 621 (D.C. Cir. 1976) (Lumbard, J., concurring). In *National Association of Regulatory Commissioners*, the D.C. Circuit denied the FCC's authority to preempt state regulation of two-way non-video communication because the FCC showed insufficient connection between its rules and the regulation of broadcasting. *Id.* at 617.

Midwest Video Corp. (Midwest Video I),[175] the FCC had promulgated a rule that cable systems serving more than 3500 subscribers had to provide some of their own programming.[176] A sharply divided Supreme Court upheld this rule under the FCC's ancillary authority, reasoning (again) that section 2(a) conferred regulatory power on the Commission.[177] Because section 2(a) did not itself "prescribe any objectives for which the Commission's regulatory power over [cable television] might properly be exercised," a test was needed for finding whether such proper objectives existed.[178] The Court found such a "test" in examining whether "long-established regulatory goals" had been met, and concluded that such an "origination rule" applied to cable systems would "further the achievement of long-established regulatory goals in the field of television broadcasting by increasing the number of outlets for community self-expression and augmenting the public's choice of programs and types of services . . . ."[179] The *Midwest Video I* Court concluded that "the regulation preserves and enhances the integrity of broadcast signals and therefore is 'reasonably ancillary to the effective performance of the Commission's various responsibilities for the regulation of television broadcasting.'"[180] Under this standard, the Commission was held to be authorized to require cable program origination since such a requirement furthered Commission policies with respect to both enhancement of local service and diversification of control of available television and cable programming.[181]

Midwest Video I thus took a giant step beyond *Southwestern Cable* in relaxing the nature of the "ancillariness" necessary to support an assertion of Commission power. *Midwest Video I* arguably turns on a determination that "ancillary to broadcasting" means not only "for the protection of broadcasting" (as in *Southwestern Cable*) but also extends to any regulation of cable which in its own right serves the purposes pursued by broadcast regulation.[182]

But the *Midwest Video I* Court sustained the Commission's jurisdiction to issue its regulations by only a 5-4 vote and without an opinion for the Court. Chief Justice Warren Burger cast the deciding vote, and, in a separate opinion, wrote that "[c]andor requires acknowledgment, for me at least, that the Commission's position strains the outer limits of even the open-ended and pervasive jurisdiction that has evolved by decisions of the Commission and the courts."[183] Though not "fully persuaded that the

175. United States v. Midwest Video Corp. (*Midwest Video I*), 406 U.S. 649 (1972).

176. Amendment of Part 74, Subpart K, of the Comm'n's Rules & Regulations Relative to Community Antenna Television Systems, 36 F.C.C.2d 143 (1972) (FCC report and order).

177. *Midwest Video I*, 406 U.S. at 661.

178. *Id.*

179. *Id.* at 667-68 (quoting Amendment of Part 74, Subpart K, of the Commission's Rules and Regulations Relative to Cmty. Antenna Television Sys., 20 F.C.C.2d 201, 202 (1969) (FCC first report and order)).

180. *Id.* at 670 (quoting United States v. Sw. Cable Co., 392 U.S. 157, 178 (1967)).

181. *See id.* at 668-70.

182. *Id.* at 662-63.

183. *Id.* at 676 (Burger, C.J., concurring in the judgment).

Commission ha[d] made the correct decision in [the] case," he was inclined to defer to its judgment.[184]

In the very next Supreme Court case about FCC ancillary jurisdiction, *FCC v. Midwest Video Corp.* (*Midwest Video II*),[185] the Court confirmed that the "outer boundary" of jurisdiction had been reached in *Southwestern Cable* and *Midwest Video I* and that the FCC had to be reined in. In *Midwest Video II*, the FCC had created rules requiring cable television systems to make available certain channels for access by public, educational, local governmental, and leased-access users, and to furnish equipment and facilities for access purposes.[186] Under these new rules, cable operators were deprived of all discretion regarding who could exploit their access channels and what could be transmitted over such channels.[187] Respondents contended that the regulations were not only qualitatively different from those heretofore approved by the courts, but that they also contravened freedom of the press guarantees—particularly the command of the Communications Act of 1934, section 3(h), (contained in the definition of "common carrier") that "a person engaged in . . . broadcasting shall not . . . be deemed a common carrier."[188]

The Supreme Court, reversing the FCC, found that the FCC's actions amounted to regulating cable systems as common carriers, and that authority for such regulation had to come specifically from Congress.[189] "Though afforded wide latitude in its supervision over communication by wire, the Commission was not delegated unrestrained authority."[190] Mere "reasonable relation" to Commission desires was not sufficient to justify ancillary jurisdiction.[191]

More recently, the FCC argued that its Title I ancillary jurisdiction justified requiring "video descriptions" for television programming,[192]

---

184. *Id.* For Chief Justice Burger, the decisive factor was that cable systems are "dependent totally on broadcast signals." *Id.* at 675. By "interrupt[ing] the signal and put[ting] it to their own use for profit, they take on burdens, one of which is regulation by the Commission." *Id.* at 676. In both the broadcast flag and IP-enabled services settings, there can be no argument that some "interruption of signal" event has occurred.

185. 440 U.S. 689, 708-09 (1979) (finding that rules requiring cable operators to provide equipment, facilities, and channel access to the public were not reasonably ancillary to FCC's regulation of broadcast and therefore were outside FCC jurisdiction).

186. *See id.* at 691-94.

187. *See id.*

188. 47 U.S.C. § 153(10) (2000).

189. *Midwest Video II*, 440 U.S. at 708-09.

190. *Id.* at 706.

191. *See id.* at 708-09.

192. Implementation of Video Description of Video Programming, 15 F.C.C.R. 15,230, 15,256-57 (2000) (FCC report and order adopting rules which mandated a certain amount of television programming with "video descriptions" per quarter). Video descriptions

> provide aural descriptions of a television program's key visual elements (such as the movement of a person in a scene) that are inserted during pauses in the program dialogue. Video descriptions change program content because they require the creation of new script to convey program details, whereas closed captions present a verbatim transcription of the program's spoken words.

Motion Picture Ass'n of Am. v. FCC, 309 F.3d 796, 798 (D.C. Cir. 2002).

noting that comments it had received demonstrated "the importance of video description to persons with visual disabilities."[193] The MPAA objected and filed suit.[194] In a crisp opinion, the D.C. Circuit reversed the FCC's determination, noting that Congress had not explicitly "authorize[d] the Commission to adopt regulations implementing video descriptions."[195] The court rebuked the FCC for its overuse of Title I, saying, "Contrary to the FCC's arguments suggesting otherwise, § 1, 47 U.S.C. § 151, does not give the FCC unlimited authority to act as it sees fit with respect to all aspects of television transmissions, without regard to the scope of the proposed regulations."[196]

B. *Breadth of FCC's Ancillary Jurisdiction Claim*

The FCC's key jurisdictional claim in both the broadcast flag and IP-enabled services rulemakings is that the Commission has regulatory authority over all interstate communication by wire or radio and all devices, facilities, apparatus, or anything else "associated with the overall circuit of messages sent and received" via wire or radio.[197] The FCC also appears to believe that it has had this power since 1934, and has simply chosen not to exercise it since then.[198]

As outlined above, in the absence of an express statutory delegation, the FCC does not have legislative rulemaking authority under Title I over all wire and radio communications within the United States and all devices concerning these communications. In both the broadcast flag and IP-enabled services contexts, Congress has clearly stated that it does not want the FCC to have the power to make detailed rules about either (1) devices that receive digital files or (2) the Internet generally.[199]

Specifically, in the All Channel Receiver Act ("ACRA"), Congress granted the FCC constrained authority to ensure that television sets receive all channels but withheld the broader power over television sets and "downstream devices" that the Commission would now like to have.[200]

193. *Implementation of Video Description*, 15 F.C.C.R. at 15,232.

194. *Motion Picture Ass'n*, 309 F.3d at 796.

195. *Id.* at 798. The D.C. Circuit also refused to accord *Chevron* deference to the FCC's determination of its powers, saying that the Commission had "acted without delegated authority from Congress" and thus *Chevron* was inapplicable. *Id.* at 807.

196. *Id.* at 798.

197. Brief for Respondents, *supra* note 71, at 17 (FCC response to the American Library Association's challenge to its jurisdiction to adopt the broadcast flag rule); *see also* IP-Enabled Services, 19 F.C.C.R. 4863, 4895 (2004) (FCC notice of proposed rulemaking) ("Title I of the Act confers upon the Commission ancillary jurisdiction over matters that are not expressly within the scope of a specific statutory mandate but nevertheless necessary to the Commission's execution of its statutorily prescribed functions.").

198. Brief for Respondents, *supra* note 71, at 25.

199. *See supra* Part II.

200. *See* 47 U.S.C. § 303(s) (2000). Originally, the All Channel Receiver Act ("ACRA") would have given the FCC broad authority to set performance standards for television receivers. *See* S. Rep. No. 87-1526 (1962), *as reprinted in* 1962 U.S.C.C.A.N. 1873, 1879. But the draft bill was sharply questioned for the role it allowed the FCC in receiver design. *Id.* Congressman Kenneth Roberts stated that "'[t]he FCC should not have the power to

Other than in the broadcast flag proceeding, the FCC has not in the past ordered non-common-carrier manufacturers to change the design of their products in the absence of a statute specifically granting the Commission authority to make such demands. Instead, the FCC has been careful not to implicitly require that particular forms of technology be installed. There are specific statutes authorizing the FCC to make rules about harmful interference from radiating devices,[201] about closed-captioning decoder circuitry (but not about specifications for such circuitry),[202] and about the V-Chip (but not about specifications for the V-Chip).[203]

In January 2004, a coalition of library associations and consumer groups sued the FCC in the D.C. Circuit, challenging the Commission's jurisdiction to adopt the broadcast flag rule.[204] In May 2005, the D.C. Circuit agreed that the FCC did not have jurisdiction over the post-receipt-of-signal operation of devices, and struck down the broadcast flag rule.[205]

As for the IP-enabled services proceeding, every one of the "social policies" proposed by the FCC is something that has been imposed in the past on telecommunications services providers—on common carriers.[206] The Commission lacks any statutory authority to impose these policies on

---

require that all sets be color sets, or have a certain size of picture tube or be made with a certain size speaker and so forth.'" Elec. Indus. Ass'n. Consumer Elec. Group v. FCC, 636 F.2d 689, 694 (D.C. Cir. 1980) (quoting *All-Channel Television Receivers: Hearing on S. 2109 before the Subcomm. on Communications of the S. Comm. on Commerce*, 87th Cong. 59 (1962) (statement of Rep. Kenneth A. Roberts)). Congress decided to "carefully limit[]" the FCC's authority only to ensure that televisions "adequately receiv[e] all frequencies." *Id.* at 692, 696. In August 2002, the FCC issued its Digital Tuner Order using ACRA as authority, directing that, on a phased-in basis starting in July 2004, all televisions sold in the United States must contain a digital tuner. Review of the Comm'n's Rules & Policies Affecting the Conversion to Digital Television, 17 F.C.C.R. 15,978, 15,996 (2002) (holding that ACRA had expressly devolved to the FCC the power to require that televisions sold in the U.S. "be capable of adequately receiving all frequencies allocated by the Commission to television broadcasting"). In late October 2003, the D.C. Circuit upheld the FCC's jurisdiction to enter the Digital Tuner Order, citing specifically FCC's reliance on ACRA. Consumer Elecs. Ass'n v. FCC, 347 F.3d 291 (D.C. Cir. 2003). This case strongly supports the notion that the FCC requires a statutory mandate in order to require non-common-carrier manufacturers to modify their devices.

201. 47 U.S.C. § 302.

202. S. Rep. No. 101-393, at 9 (1990), *as reprinted in* 1990 U.S.C.C.A.N. 1438, 1446.

203. *See* 47 U.S.C. §§ 303(x), 330(c). Again, these provisions of the act were not technology-specific, and authorized the FCC only to require manufacturers to equip televisions with "a feature designed to enable viewers to block display of programs carrying a common rating." H.R. Rep. No. 104-458, at 196 (1996) (Conf. Rep.), *as reprinted in* 1996 U.S.C.C.A.N. 10, 210. In doing so, Congress instructed the FCC to preserve for manufacturers the option of using "alternative technology that meets certain standards of cost, effectiveness and ease of use." *Id.*

204. Susan P. Crawford, *The Biology of the Broadcast Flag*, 25 Hastings Comm. & Ent. L.J. 603 (2003).

205. *See* Am. Library Ass'n v. FCC, 406 F.3d 689 (D.C. Cir. 2005).

206. "The Commission has concluded, and courts have agreed, that the 'telecommunications service' definition [found in the Communications Act] was 'intended to clarify that telecommunications services are common carrier services.'" IP-Enabled Servs., 19 F.C.C.R. 4863, 4880-81 (2004) (FCC notice of proposed rulemaking) (quoting Cable & Wireless, PLC, 12 F.C.C.R. 8516, 8521 (1997) (FCC cable landing license order)).

non-common carriers. Indeed, Congress, in Section 509 of the same Communications Act, which the FCC is charged with administering, explicitly elected not to impose common carrier obligations on interactive computer services,[207] as described in Part I above.

C. *Extension of CALEA to the Internet Is a Statutory Impossibility*

Perhaps aware that its "ancillary jurisdiction" claims were insufficiently strong to withstand litigation in the broadcast flag and IP-enabled services settings, the Commission has not relied on this theory in the CALEA context. Instead, the FCC has used a novel reading of the CALEA statute to support its argument that CALEA should be extended to the Internet. CALEA states that the term "telecommunications carrier" (the entities covered by CALEA) includes "a person or entity engaged in providing wire or electronic communication switching or transmission service to the extent that the Commission finds that such service is a replacement for a substantial portion of the local telephone exchange service . . . ."[208] CALEA then excludes from the definition of "telecommunications carrier" all "information services."[209] The Commission has interpreted the "substantial replacement" language of CALEA to cover both provision of any kind of broadband Internet access service and "interconnected" VoIP services,[210] and has ignored the overarching "information services" exclusion—effectively reading this exclusion out of the statute.

As discussed above, CALEA was a narrowly drawn statute focused carefully (after much negotiation) on the traditional telephone system, and the "information services" exclusion from the scope of CALEA was intended to be broadly read. The Commission has no authority to redraw the outlines of CALEA's application to include either Internet access or Internet applications. Only Congress can take this step.[211]

V. INFORMATION FLOWS AND COMPLEX SYSTEMS

Once we are back in Congress to talk about regulating the Internet in order to assist law enforcement, the content industry, and incumbent

207. 47 U.S.C. § 230 (2000).

208. *Id.* § 1001(8)(B)(ii).

209. *Id.* § 1001(8)(C)(i).

210. Communications Assistance for Law Enforcement Act, 69 Fed. Reg. 56,976, 56,798 (Sept. 23, 2004) (to be codified at 47 C.F.R. §§ 22, 24, 64).

211. The Commission's belief in its "unregulation" agenda for IP-enabled services received substantial support in the Supreme Court's recent opinion in *National Cable & Telecommunications Association v. Brand X Internet Services*, 125 S.Ct. 2688 (2005). The Court said in dicta that although "information-service providers . . . are not subject to mandatory common-carrier regulation under Title II . . . the Commission has jurisdiction to impose additional regulatory obligations under its Title I ancillary jurisdiction," and indicated that policy in this "technical and complex" area should be set by the Commission (and thus impliedly not by the courts or Congress). *Id.* at 2696, 2705. The *Brand X* opinion can fairly be read to give the Commission complete discretion over what rules should be mandated with respect to "information services" (including the Internet), even if those rules are the same as rules applied to common carriers.

telephone companies, what should we say? It is not enough simply to claim that "the Internet is different" and that therefore Congress should keep away.

This part presents the claim that the Internet is a complex system. Insofar as governments care (as they should) about the benefits of the information flows made possible online, the complexities of these existing membranes will defeat large-scale governmental intervention. The best way to proceed is to facilitate the evolution of complex small-scale regulatory mechanisms that themselves provide social order.

A. *The Internet as Complex Environment*

The Internet is itself a complex system, made up of many interacting agents (including many non-state communities) whose dynamic engagements produce elaborate permeable membranes regulating information flow.[212] Complex adaptive systems, such as the Internet, economies, weather, and social organizations, are based on the actions of autonomous agents that act to maximize their "fitness" (or success as measured against a particular landscape) over time. These agents also communicate with their neighbors. This structure produces responses that are neither predictable nor linear. Interactions among these agents lead to emergent properties of the system—properties that could not be explained by traditional analysis—that are not properties of the agents themselves. And the actions of these agents distort or deform the "fitness landscape" that provides the system's environment, making it a very rugged landscape indeed. Two key concepts will help us think about the Internet's particular complexities: "scale" and "patching."

1. Scale

Complex systems are more or less complex at different scales. Indeed, every complex system is a tradeoff of complexity at one scale (e.g., lots of complexity at a fine scale, with actions at that scale characterized by independence and randomness) in exchange for less complexity at another scale (e.g., little complexity at a higher scale but greater ability to act coherently and interdependently). An ancient army was fairly complex at a large scale—but only because all of its soldiers had little autonomy at a fine scale. In contrast, an unruly mob is complex at a small scale. Every member of a mob can do whatever he wants. But collectively, mobs cannot do anything very complex—they can storm a castle, but cannot organize the resources inside the castle very effectively.

The environments of complex systems are also complex. For example, from the perspective of a rabbit, his environment is itself a complex system, full of autonomous agents (other animals, barriers) and interdependence (predator-prey relationships, food availability). Both systems and

212. *See generally* Albert-Laszlo Barabasi, Linked: The New Science of Networks (2002).

environments are complex systems with tradeoffs in complexity at different scales.

We know that the collective complexity of a traditional hierarchical organization—the number of possible states that an organization can be in—can never exceed the complexity of the individual at the very top.[213] That person has limited bandwidth; literally, he can only take in and give out a finite amount of information. The problem is that the environment of an organization may become more complex than the complexity of the individual at the top of the organization's hierarchy. When that happens, when there is a mismatch between the complexity of an organization and the complexity of the organization's environment, the organization will (over time) fail. The organization will now be in an environment that is too complex for it to exist.

Similarly, because centralized control attempts for any moderately complex environment are likely to be less complex than that environment, they are likely to fail. Think of the food supply for New York City. What if someone decided that having seventy sources of mushrooms was inefficient because some people were unable to have access to all the varieties of mushrooms they wanted, and others had mushrooms on hand that they did not need? That same person could institute a centrally planned system that would take careful account of what everyone needed and what was available, and would ensure that very large quantities of inexpensive (but high quality) mushrooms would be made available by a single supplier to restaurants all over the city. The same person, or bureau, would make decisions about fish and arugula and soy sauce and everything else the city needed. All fair prices, all planned to the smallest detail. What would happen?

We would have shortages and long lines all over the city. This is, indeed, what happened to the Soviet central planners, whose multiple five-year plans resulted in economic stagnation.[214] The Russian system could not adapt to the many changes in its environment. Central planning of a complex system, with its many inputs and interdependencies, will not work, and will be particularly unsuccessful when the system is operating in an uncertain environment whose complexity exceeds that of the system.

Just as there needs to be a mapping between the complexity of a system and the complexity of its environment, complexity at different scales becomes a crucial consideration for system/environment interactions. Systems that operate at a large scale will defeat small scale environmental

213. Yaneer Bar-Yam, *Multiscale Variety in Complex Systems*, Complexity, Mar.-Apr. 2004, at 37.

214. Mikhail Gorbachev, Perestroika 17-19 (1987).

> Analyzing the situation, we first discovered a slowing economic growth . . . to a level close to economic stagnation . . . . A country that was once quickly closing on the world's advanced nations began to lose one position after another . . . [in] scientific and technological development, [and in] the production of advanced technology.

Id. at 19.

complexity if these two systems are able to meet. Thus, for example, if there are no other impediments an elephant can flatten a person and a tank can flatten a forest. But if a large-scale system is confronted with barriers to its operation, it will be defeated by small-scale complexity. So, for example, if a tank wanted to move through a forest to get to the next town, but the tank manager was concerned about the health of the forest and was reluctant to knock down individual trees, the tank's large-scale motions would be frustrated by the small-scale complexity of its environment.

The U.S. experience in Iraq is illustrative: The U.S. army was perfectly good at marching into ("flattening") Baghdad, but the post-intervention maintenance of order in Iraq—which requires enormously complex interactions with people whom we have no interest in flattening—has been beyond the capabilities of the forces that are on the ground there. By contrast, the U.S. campaign in Afghanistan (which used autonomous Special Forces troops to deal with the complex situation on the ground) was relatively successful. Large-scale, simple moves by a particular system will be defeated by the complexity of that system's environment if the two are unable to engage, for whatever reason.

When one thinks of the Internet as a complex system/environment in which government is attempting to operate, the problem becomes clear. The Internet is like the terrain on which a battle is being played out, and it is an extraordinarily complex landscape. There are many many possible states of information flows and membranes online, and more are developing every day. Otherwise stated, the number of possibilities for the states of information flows online—the online environment's complexity—is very high indeed. But governments, as rulemakers, are usually rigidly hierarchical. Thus, their organizational ability to make decisions is only as complex as the bandwidth of the person at the top of the relevant hierarchy. Again, where the complexity of a system (government) is insufficient to cope with the complexity of its environment (the Internet), the system will be unsuccessful.

Let us assume that governments plan to mandate large-scale information flow membranes for the Internet ("this unlawful bit shall not pass this technical barrier"). What will happen? There are two answers. First, if governments act on a very large scale, they can simply defeat the complexity of information flows online. The online world provides opportunities for governmental informational control that have never been available offline. Code is very difficult for an average citizen to disobey. If all the devices that connect to the Internet are constrained by government mandate, and all applications are monitored by governmental authorities, there will be no opportunities for the creation of private membranes that permit the further explosive evolution of social and cultural life online. The mandated membrane (the tank) can flatten the membranes that now exist (the forest). Indeed, China has on a large scale taken on exactly this task,

by creating a border-membrane through which all Internet communications must flow.[215]

The second answer is that although large scale operations can certainly defeat complexity when the large-scale system is able to operate, the complexity of the Internet's existing information flow structures (many elements of which governments will want to retain for their positive benefits) will ultimately make it impossible for governments to act successfully in establishing their own membranes—particularly if they have any concerns at all about downstream effects. The complexities of the Internet's existing information flow structures produce many positive benefits for governments. Among many other things, economic growth—including increased productivity, creation of jobs, and higher wages—is spurred by Internet connectivity and the creation of membranes across physical, geographical borders. The Internet is not (just) a sea of pornography; it makes it possible for tiny businesses in remote villages to sell their wares and learn about space travel. There are, in fact, many positive affordances of the Internet that are created by the availability of decentralized information-flow management. Flattening the complexity of the Internet's information-flow membranes may have complex downstream effects that are impossible to predict and are not ultimately beneficial to governments.[216]

In other words, scale can win out over complexity only if they can encounter each other. Because no government will want to completely flatten the Internet's non-state membrane structure, efforts to constrain the information flows of the Internet by centralized means will ultimately be frustrated by the complexity of information flows online.

---

215. Jonathan Zittrain & Benjamin Edelman, *Internet Filtering in China*, IEEE Internet Computing, Mar.-Apr. 2003, at 70, *available at* http://cyber.law.harvard.edu/filtering/china/.

216. Applying large-scale "fixes" to online information flow membranes is roughly similar to sending a medication into the complex system that is the human body. Medical researchers know that drugs work by binding to a protein, and usually by inhibiting the actions of that protein. Many in the past believed that one could change the human body by targeting a single protein and causing cells to move from one state—e.g., death—to another (e.g., proliferation). It turns out, however, that proteins targeted for blocking are themselves part of a network of communicating proteins. So, for example, Vioxx inhibits a protein called COX-2, which causes pain. But, downstream, COX-2 supports vasoconstriction and decreases the risk of heart attacks. So Vioxx is a double-edged sword, and has had to be withdrawn from the market. Marc Kaufman, *Merck Withdraws Arthritis Medication*, Wash. Post, Oct. 1, 2004, at A1, *available at* http://www.washingtonpost.com/wp-dyn/articles/A63157-2004Sep30.html. Similarly, large-scale membranes designed to "inhibit" one kind of information flow online will inevitably have unpredictable, amplified, and possibly conflicting effects down the road. The recent case *Center for Democracy & Technology v. Pappert*, 337 F. Supp. 2d 606 (E.D. Pa. 2004), in which a Pennsylvania state statute instructing ISPs to block child pornography sites resulted in the blocking of more than a million innocent and lawful sites, illustrates the risks of large-scale online information flow membrane management. *See* Grant Gross, *Court Rules Against State Web-Blocking Law*, PC World, Sept. 10, 2004, at 10, *available at* http://www.pcworld.com/news/article/0,aid,117740,00.asp.

2. Patching

In an environment full of conflict and nonlinear dynamic change, it is very difficult for a complex system to "find" the global, overall optimum for the system as a whole. There are simply too many choices to make and too much wasted time spent wandering the landscape. Systems attempting to find compromises that will be best for all their actors will often get stuck on metaphorically "low" hills. Like a drop of water or a ball, they stop searching for anything "better" once they stop rolling, because any other step against their dynamic, unpredictable landscape may lead suddenly to a destabilizing avalanche. The system, in Stuart Kauffman's words, is "caught in a web of conflicting constraints" in which "each small part of the system affects other parts of the whole system, [and] changing [the state of a single element] will have effects that ripple throughout the system."[217] The risk of acting in ways that will be harmful is great.

How could management do better? It turns out that they can do better by diversifying. As David G. Post and David R. Johnson have explained (drawing on the work of Stuart Kauffman),[218] when systems are divided into patches and agents' actions are measured and responded to with respect to their effect on the aggregate fitness of their respective patch (rather than on the system as a whole), the system as a whole will find its way more efficiently towards an optimum position.[219] In effect, permitting selfish patches to act in their own self-interest permits the system to "fail" temporarily—to move to a lower point on the fitness landscape, which then allows ascent to a higher peak after further moves. Post and Johnson have also shown that there is a level of spillover effect, or mapping between the welfare of a particular patch and its effect on outsiders, which will lead to more optimal overall results. They called this measure of spillover "congruence."

Thus, deferring to every individual membrane would not lead to social order. Deferring to a single authoritative source of membranes would lead to a frozen, lifeless tundra. Stuart Kauffman, as interpreted by Post and Johnson, has shown us that having a single source of membranes in this conflict-ridden online landscape would not lead to the best results. Indeed, such a single patch would inevitably freeze in its tracks on a foothill in the fitness environment. For optimal results, complex systems should be divided into competing, co-evolving (and sometimes selfish) patches. From the Internet perspective, one can think of these patches as sets of rules (or membranes) permitting particular information flows.

Congress should restrain itself in the name of evolution by listening to the same intuitions that gave us the healthy, thriving Internet we have

---

217. Stuart Kauffman, At Home in the Universe: The Search for Laws of Self-Organization and Complexity 173 (1995).

218. David G. Post & David R. Johnson, *"Chaos Prevailing on Every Continent": Towards a New Theory of Decentralized Decision-Making in Complex Systems*, 73 Chi.-Kent L. Rev. 1055 (1998).

219. *Id.* at 1059-60.

today. Congress should recognize the scaling issues that will make intervention difficult, and permit the "patching" of rules by facilitating the continued development of private information flow membranes online.

CONCLUSION: THE MESSY GLOBAL LANDSCAPE

Internet governance is, in reality, focused on regulating information flows and not at all with traditional "governance" of behavior by governments. These information flows, in turn, are occurring within a complex environment—the Internet—whose dynamics are nonlinear and unpredictable. If information flows are the subject of Internet governance, how should they be governed?

We know that most large top-down engineering projects fail because they are simply too complex, and that centralized approaches to these projects will not work.[220] We also know that large-scale, simple approaches to complex environments will fail if their ability to operate is frustrated; online, because there are many information-flow membranes that are valuable to governments, large-scale governance efforts will never succeed.[221] Finally, we know that evolution produces contextual "solutions" to these hard engineering problems.[222] We thus have two choices: to avoid altogether the complex task of working on information flows, or to allow "better" membranes to emerge through evolution. Because governments will not be content with simply leaving information flows alone, they will need evolutionary guidance to encourage the development of highly evolved membranes.

The great choice we face at this moment in the history of the Internet is that there are very powerful forces at work—law enforcement, telecommunications companies, and the content industry—who would like to see mandated membranes and gateways of all kinds erected to block particular bits online. These industries are demanding exactly the kind of large-scale, tank-flattening-the-forest kinds of initiatives that pose great risks to the future of online life because they will stifle continued evolution. We need to point out to legislative bodies that online life is already highly structured. Patches abound. Non-state groups are arising that are creating their own membranes for information flows, and there is a real marketplace

220. Yaneer Bar-Yam, When Systems Engineering Fails—Toward Complex Systems Engineering, http://necsi.org/projects/yaneer/E3-IEEE_final.pdf (last visited Oct. 23, 2005). A 1995 study by the Standish Group showed that an astounding 30% of large U.S. engineering projects were scrapped, 50% went nearly 200% over cost, and 20% were "challenged"—fraught with difficulties. The Standish Group, Chaos (1995), *available at* http://wwwbroy.in.tum.de/lehre/vorlesungen/vse/WS2004/1995_Standish_Chaos.pdf.

221. *See supra* Part I.

222. Bar-Yam, *supra* note 220; *see* Barbara A. Cherry, Office of Strategic Planning and Policy Analysis, Fed. Commc'ns Comm., The Telecommunications Economy and Regulation as Coevolving Complex Adaptive Systems: Implications for Federalism, *available at* http://quello.msu.edu/complexity/CherryTPRC04.pdf (last visited Oct. 23, 2005); J.B. Ruhl, *Thinking of Environmental Law as a Complex Adaptive System: How to Clean Up the Environment by Making a Mess of Environmental Law*, 34 Hous. L. Rev. 933 (1997).

of ideas online that allows these groups to act as civic organizations.[223] Vast numbers of people are online and are participating in evolving and value-creating information exchanges of all kinds. (Indeed, one of the primary engines behind calls for Internet governance is not a quest for governance at all, but rather the desire of developing nations to be online at lower costs than are currently permitted by global settlement regimes.) The online world is no longer the Wild West and may never have been.

It is true that there are forces of informational destabilization that are perceived to be at work. Spam is often cited as one of these forces; some people will say that email has become useless because of the seething flood of unwanted messages being propagated across the Internet. Security threats generally are viewed as enormous problems online, with viruses and hacking attacks becoming central concerns of businesses and governments. Terrorists are using the Internet to plan their attacks (just as they would use any method of communication available to them), and law enforcement agencies would like the power to be able to listen in easily and to retain all possible communications among the bad guys. Fraud is viewed as a problem that is more prevalent online than offline. Peer-to-peer file trading is also viewed as destabilizing, particularly to a content industry that has heretofore been able to control distribution windows for its works.

Each of these incrementally destabilizing phenomena is viewed by some to be capable of causing an electronic natural disaster—an avalanche of bits. We know from complexity theory, however, that the risk of an avalanche is one we have to take in order to obtain the benefits of a dynamic, communicating, evolving, optimal system. We also know that we are more likely to get that optimal system if we allow communities and groups of all kinds to build their own patch membranes. This is, in a sense, the lesson of federalism, and federalism that includes a role for online non-state communities is what is needed for the Internet. The harmonized rule of law, in this bit-based setting, is not as important as respect for the cultures and societies that are emerging online.

If we allow a diverse set of communities to adopt their own rules and make their own decisions about their own two-way membranes (allowing and blocking flows of information), we will facilitate the co-evolution of patches toward a better overall result. Central planning regarding the permeability of information membranes—whether replication or amplification of bits is permitted across a particular boundary—can never work as well. The only available strategy to create a good society has been to allow valuable membranes to evolve. These membranes include civic groups, innovative economic action, constructive social collaboration, and many other things that make up civic life. Because the nature, intensity, and content of information flows online will continue to change, and because the desires of individuals and the nature of the groups they join will

223. Noveck, *supra* note 24, at 5 ("We should explore ways to structure the law so as to circumscribe malevolent groups while deferring political and legal decisionmaking to decentralized group-based decisionmaking.").

continue to evolve, we need to be friendly to conditions that permit optimal flexibility and facilitate evolution of permeable information-flow membranes. We may experience some temporary avalanches along the way, but the membranes that emerge will evolve to fit the landscape. We will never be stuck.

Somehow, the perception that the Internet is a machine constructed out of tangible hardware and binary software code has led to a view that it can be regulated by a machine. But the real Internet, the one that matters, is as interesting as society itself. It could no more be governed by a centralized authority than could a good conversation. In a larger sense, we clearly still need governments to prohibit (offline) murder. But the targeted regulation of the bad behavior of bad actors is a kind of activity that is very different from efforts to control where bits flow. We have never willingly looked to governments to control information flows, because decentralized actions by diverse individuals and groups are clearly much better suited to take on this highly complex task.

Once we understand the importance of membranes and the impossibility of designing them in advance, the desirability of facilitating evolution as the key global legal and political goal for Internet governance is clear. Information flow membranes will get "better" by co-evolving—adapting, through feedback and continuous change to a world filled with other complex systems with which they have to interact. Our social institutions, our collective information flow membranes, must be allowed to evolve to become as complex as necessary to permit the most valuable and interesting society to emerge. Given what we know about complex networks, the course of this evolution will tend towards heterogeneity, not homogeneity.[224]

Congress needs to show leadership at this moment by reasserting its hands-off, "unfettered by federal or state regulation" approach—which is an "evolutionary" approach to permeable information flow membranes stated in legislative language—to the Internet. There is still a chance that if Congress takes a cosmopolitan[225] approach to Internet governance it will be able to persuade other agencies around the world to restrain their regulatory desires despite the entreaties of law enforcement, the content industry, and telecommunications companies. The natural state of the cosmos, and of the Internet, is not chaos. It is, instead, order, that comes about with no external pilot. But this kind of lively, dynamic order only emerges when it

224. The Dawkins gene-centered view of the world is wrong. *See generally* Richard Dawkins, The Selfish Gene (1990). "In fact, spontaneous pattern formation in the presence of disruptive selection increases the generation and duration of genetic diversity." Erik M. Rauch et al., NECI Research Projects, Evolution and Ecology, http://necsi.org/projects/sayama/evolecol.html (last visited Oct. 23, 2005).

225. Paul Schiff Berman has persuasively argued for a "cosmopolitan" view of Internet jurisdiction, attempting to locate jurisdictional middle ground between strict territorialism on the one hand and expansive universalism on the other. Paul Schiff Berman, *The Globalization of Jurisdiction*, 151 U. Pa. L. Rev. 311, 490-512 (2002).

is permitted to do so. The next step in Internet governance should be to take the long view.