The Ambulance, the Squad Car, and the Internet

by
SUSAN P. CRAWFORD*

* Associate Professor, Cardozo School of Law. Thanks to Yochai Benkler, John Brown, Julie Cohen, William Fisher, Brett Frischmann, Michael Herz, Molly van Houweling, David Johnson, Mark Lemley, Michael Madison, John Morris, Margaret Jane Radin, Pam Samuelson, Christopher Springer, Kevin Stack, Stewart Sterk, Rebecca Tushnet, Kevin Werbach, Rick Whitt, Christopher Yoo, and Jonathan Zittrain. Earlier versions of this paper were presented at the 2005 Berkman cyberprof retreat, the Berkeley Intellectual Property Scholarship Seminar, and the Wharton Colloquium on Media and Communications Law.

INTRODUCTION

The Federal Communications Commission moved swiftly in 2005 to impose E911[1] and CALEA[2] requirements—two "social policies"[3] that had been applied to telephone companies—on broadband internet access providers and online applications. E911, broadly speaking, requires telephone companies to provide location information to a dedicated call center for anyone calling 911; CALEA, in general, requires telephone companies to design their services so as to be easily tappable by law enforcement In the E911 context, dominant vendors of outsourced E911 compliance services have caused the FCC to insist that online businesses find ways to make their services work with 30-year-old legacy emergency hardware (access to which is controlled by the vendors). In the CALEA context, law enforcement has persuaded the Commission to rely on extraordinarily weak legal arguments in insisting that online businesses and broadband access providers make their services acceptable to law enforcement—either before these services are launched, thus constraining innovation, or for existing services at great retrofitting expense. In both settings, the FCC has plunged quickly ahead to apply these policies to the internet with little consideration either for the economic impacts of its

1. *In the Matters Of IP-Enabled Services and E911 Requirements for IP-Enabled Service Providers*, WC Dkt. Nos. 04-36 and 05-196, *First Report and Order and Notice of Proposed Rulemaking*, rel. Jun. 3, 2005 [E911 Order]. The E911 Order required providers of "interconnected VoIP" services (roughly, Voice over Internet Protocol (online) services that connect to the traditional telephone network) to make traditional 911 access available to their subscribers by November 28, 2005.

2. *In the Matter Of Communications Assistance for Law Enforcement Act and Broadband Access and Services,* ET Dkt. No. 04-295, RM-10865, *First Report and Order and Further Notice of Proposed Rulemaking*, rel. Sept. 23, 2005 [CALEA Order]. The CALEA (Communications Assistance for Law Enforcement Act) Order states that providers of interconnected VoIP services and broadband internet access are required to comply with CALEA by May 2007 by making their applications and facilities easily tappable by law enforcement.

3. The Commission uses the term "social policies" as a blanket descriptor for a list of regulations that have been applied to traditional telephones and are not related to the rates charged for particular services. *See In the Matter of IP-Enabled Services,* WC Dkt. No. 04-36, Notice of Proposed Rulemaking, rel. Mar. 10, 2004 ("IP NPRM"), at ¶ 36: "We thus focus primarily on ways to distinguish services that might be viewed as replacements for traditional voice telephony (and which thus raise *social policy* concerns relating to emergency services, law enforcement, access by individuals with disabilities, consumer protection, universal service, and so forth) from other services (which do not appear to raise these same regulatory questions to the same extent.") (emphasis supplied). *See* Susan P. Crawford, *Shortness of Vision*, 74 Fordham L.Rev. 695 (2005) (describing IP NPRM and "social policy" approach in global context of internet regulation).

choices or for alternative strategies that might have been employed. And both policies have been lifted largely unchanged from what they had been in the world of telephony, even though the internet presents a very different technical and economic context.

These proceedings, taken together, provide a case study in a new form of digital era regulatory capture. Where an independent agency believes it has a broad delegation of power over new technology from Congress, and has a political agenda and the technical assistance of dominant unregulated entities intent on retaining the advantages that the old technology gave them—in this case, assistance came from providers of outsourced compliance services to telephone companies, and from the Department of Justice, a powerful sister agency—incumbents can easily use regulation to raise the costs of entry for new competitors. Unlike the usual tale of regulatory capture, the work of FCC staff on these rulemakings was not necessarily corrupt, and can be explained in part by the cultural background of staff (their traditional telephony or "bellhead" orientation). But the interplay among the key players in this new form of capture has resulted in a toxic environment for new online businesses established to compete with traditional telecommunications providers: The combination of hard social questions, the ever-present threat of terrorism, captured but well-meaning staff, law enforcement heavy-handedness, dominant vendors of compliance services, and well-funded activities of rent-seeking incumbents has resulted in substantial barriers to entry being created for a significant portion of the American economy by an unaccountable independent agency. The application by the FCC of E911 and CALEA policies to the internet has already sparked lawsuits.[4] Although there are as yet no judicial opinions on these matters, a line from an article by Prof. Thomas Merrill encourages me to proceed: "Legal scholars who take their cues from courts will always end up playing 'catch-up,' attempting to integrate judicial innovations with previously established understandings and (perhaps) with social science literature. But they will rarely serve as catalysts for change."[5] This Article tells the story of this new form of regulatory capture, and is aimed at galvanizing Congressional action to constrain the Commission's currently apparently unlimited discretion to regulate the internet.

4. American Council on Education et al. v. FCC, 05-1404 (D.C. Circuit 2005) (multiple consolidated cases challenging CALEA Order); Nuvio v. FCC, 05-1248 (D.C. Circuit 2005) (challenging E911 Order).

5. Thomas Merrill, *Capture Theory and the Courts*, 71 Chi.-Kent L. Rev. 1039, 1067 (1997).

The early rulemakings I discuss in this Article rely on assumptions: we are in a new age, *and therefore* social policies from the old age need to be brought forward into this new age. We are referred back, ceaselessly, to the need to assuage fears about emergency services and law enforcement access—to bring in the ambulance and the squad car—without much analysis. The FCC says only that it wants to provide a "level playing field" for the digital age by treating everyone alike in implementing these "social policies" online. It is requiring that these policies be carried out in a centralized, unitary, command-and-control fashion well-suited to the world of telephones. But the internet should have taught us, by now, that there are alternative ways to reach our social policy goals. The argument is not that the new actors discussed in this Article should be exempt from emergency and law enforcement concerns. Although there is a case to be made for that argument, it is a case that is politically untenable, and I do not advance it here. My argument instead is that by insisting that these actors pursue these ends by the same means as traditional telephone providers, we have both missed crucial opportunities and imposed heavy costs on new market entrants. In addition to outlining the case studies of regulatory capture provided by these proceedings, this Article examines the alternative routes that Congress might want to follow in the future.

To describe the capture case studies and suggest alternative routes requires some groundwork. Part I lays out the social concerns that underlay both the E911 and CALEA rulemakings, describes the history of both of these efforts and the dynamic cooperation between third-party vendors of outsourced services, law enforcement/public safety officials, and staff, and details the enormous implementation difficulties that have been caused by the FCC's rush to impose these social policies on online businesses.

These two rulemakings are at different stages. In the E911 context, the third-party outsourced service providers and incumbent telephone companies have successfully managed to cause the FCC to create a standard that serves their business interests and puts their competitors out of business; in the CALEA context, law enforcement has managed to cause the FCC to create a legally-tenuous threat of compliance liability without saying what compliance actually entails.

Part II sketches the market context for the E911 and CALEA rulemakings by introducing the *dramatis personae* involved in both proceedings. In brief, incumbent telephone companies are being daily

undermined by the success of new online services; vendors of compliance services to traditional telephone companies are looking for new market niches to serve; and law enforcement and emergency services authorities are longing for the relative simplicity of the days of telephony. Part III compares the case study of regulatory capture provided by these rulemakings to prior capture narratives, and suggests that we have moved into a new era of regulatory capture in the digital era. Part IV outlines alternative ways in which the social policies embodied in the E911 and CALEA rulemakings might be implemented, and what role Congress should take at this pivotal moment in the short history of the internet.

I. THE MARKET CONTEXT

Ten years ago, when the Telecommunications Act of 1996 was passed, few people had heard of "broadband" and telephone companies were selling telephone services. Today, the telephone companies are angling to provide television services, and according to the FCC 38 million Americans (about 60% of active internet users in the U.S.) have broadband access.[6]

In this new world, the nation's Baby Bell telephone companies—Verizon, SBC, BellSouth, and Qwest, the companies remaining from the seven original Baby Bells that were created in 1984 with the breakup of AT&T—have been struggling, cutting jobs and losing market value. They are losing local wireline (traditional) telephone customers to VoIP and wireless services at a rate of about 5% of their basic phone subscribers each year.[7] According to a September 2005 report, six percent of U.S. households now have *only* wireless phones.[8] Since 2000, the number of

6. FCC Press Release, *Federal Communications Commission Releases Data on High-Speed Services for Internet Access*, Washington, D.C., Jul. 7, 2005. Internet access speeds are measured by kilobits per second (kbps) and megabits per second (mbps). The FCC's claims about U.S. broadband access have been sharply disputed, because the FCC considers anything over 200kbps to be "broadband." *Id*. *See* Freepress, Consumers Union, Consumer Federation of America, *Report: Broadband Reality Check*, rel. Aug. 2005, *available at* http://www.freepress.net/docs/broadband_report.pdf. This speed is too low to *receive* low-quality video, much less originate high-quality video. *Id*. For comparison, dial-up speed is around 56kbps. The International Telecommunication Union (ITU) reported that in 2005 the top five nations for broadband network market penetration were Korea, Hong Kong, the Netherlands, Denmark and Canada. The ITU ranked the United States sixteenth in broadband penetration. *Id*. at 4.

7. Jon Arnold, *The IP Heat is On*, Telecommunications Am., Feb. 14, 2005 (2005 WLNR 4973909); Leslie Cauley, *BellSouth Likes To Go It Alone*, USAToday, Nov. 1, 2005.

8. The Insight Research Corporation, *Fixed Mobile Convergence: Single Phone Solutions for Wireless, Wireline, and VoIP Convergence, 2005-2011*, Sept. 2005 Exec. Summary, at 1.

wireline subscribers has fallen by 13.5 million, to 178 million in 2005.[9] SBC and Verizon lost 1.3 million and 3 million access lines, respectively, between June 30, 2004 and June 30, 2005.[10]

These Baby Bell difficulties relate to the growth of VoIP usage in the U.S.[11] Although the idea of offering voice services online is not new, and Net2Phone and others have been selling voice services since 1996,[12] only the availability of broadband access and special VoIP equipment has made these services truly attractive to consumers. The uptick in VoIP usage began in 2002, when 50-employee Vonage Holdings Corp. offered a much cheaper internet-based voice service that worked through telephone-like handsets connected to adapters that could packetize voice. Consumers were delighted not to have to talk into their PCs.

Vonage and other VoIP services can offer voice services more cheaply than traditional telephone companies can because Vonage customers do not have to pay the taxes and access fees associated with traditional phone service offered by the Baby Bells.[13] Vonage, advertising itself as The Broadband Phone Company and using ads that poked fun at people who paid too much for phone service, has grown quickly since 2002, and now has 1500 employees and a million subscribers.[14] And free or nearly free voice offerings from Skype, Yahoo!, MSN and Google complicate things further for the Bells.[15] Ebay's recent purchase of Skype is increasing the risk that Skype, with its 49 million users worldwide, will be a powerful player in North America, although it has only about 260,000 paying users now.[16] VoIP services in general are growing quickly. There are now between 2 and 3 million VoIP subscribers in the U.S., and there are projected to be between 12 and 40 million by 2011.[17]

9. Elizabeth Wasserman, *The New Telecom Wars: Looking to Update a Landmark Law*, CQ Weekly, Nov. 11, 2005.

10. Mike Farrell, *Dialing Without Dollars: Price Pressures Could Wring Profit Out of Cable's Booming Telephone Business*, Multichannel News, Oct. 3, 2005.

11. There are other reasons for the decline in the incumbents' number of telephone lines and subscribers. These reasons include: (1) the rise of cell phones, (2) the obsolescence of fax lines, (3) the obsolescence of dial-up internet service, for which many people picked up (and then dropped) an extra phone line, and (4) substitution of email and instant messaging communications for telephone calls.

12. *See* About Net2Phone, http://web.net2phone.com/about/.

13. Tom Johnson, *Calling the Shots and Holding the Line*, Aug. 16, 2005.

14. Shawn Young, *Talk is Too Cheap: VoIP Profits Grow Scarce*, (Toronto) Globe and Mail, Aug. 26, 2005.

15. eWeek, *Big Players Enter VoIP Game,* Sept 20, 2005.

16. Multichannel News, *supra* n. 10.

17. Joyzelle Davis, *YoIP Battle Heats Up*, (Denver) Rocky Mountain News, Nov. 7, 2005;

All of this activity has forced some striking price reductions in online voice services. Vonage cut its prices by nearly 30 percent in 2004. Several cable companies have entered the online voice market by offering bundles of services at heavily discounted prices.[18] The Bells are hoping to survive this price-cutting, as they survived the long-distance price wars in the 1990s.[19] And the Bells are beginning to launch their own VoIP plans. For example, AT&T initiated its online voice product, called CallVantage, in April 2004, and charged a flat rate of $40/month that included all types of calls.[20] Vonage lowered its own monthly rate in response.[21] Verizon is now offering VoiceWing to customers for $35 a month, and Vonage, AT&T and Verizon have all introduced even lower-cost plans. Voice service online is becoming essentially free.

With one of their key business areas slipping away, the Baby Bells are looking for an operating plan that will allow them to survive. They are betting that even if voice is essentially free, consumers will pay for packages that include on-demand movies and other video services plus voice and data. The Bells believe—possibly rightly—that consumers would like to receive only one bill for all the communications services they use, and that online video services controlled by the access provider will be attractive to their subscribers. In effect, the Bells are planning to combine all of their offerings on a single network instead of having separate networks for telephone, cell phone, internet and television services, so that users could get to their email from their television sets or any other network device, and see caller ID information on any device whenever the phone rings.[22] Throughout most of 2005, therefore, the Baby Bells bombarded the nation with advertisements for packages that included landline and wireless voice products, VoIP, internet access, and video services. They also began pushing for legislation that would allow them to offer "premium" services (giving access to these packages) to their customers.[23]

Multichannel News, *supra* n.10; USAToday, *supra* n.7.

18. Globe and Mail, *supra* n.13.

19. *Id*.

20. *Id*.

21. *Id*.

22. John Roper, *FCC Puts Off Merger Votes,* Houston Chronicle, Oct. 29, 2005.

23. *See* Declan McCullagh, *Playing Favorites on the Net?*, News.com, Dec. 21, 2005 ("A bill expected early next year in the U.S. House of Representatives, coupled with recent comments made by executives from BellSouth and the newly merged AT&T and SBC Communications, has raised the prospect of a two-tiered Internet in which some services--especially video--would be favored over others.")

In order to be confident that consumers will be willing to pay for these packages, the Bells have worked very hard to ensure that their networks will not be subject to common carriage or nondiscrimination obligations that might force these network managers to carry competing voice or video services (such as Skype or GoogleVideo). Immediately following the summer 2005 BrandX decision,[24] which made clear that cable networks had no common carriage obligations, the Bells demanded that DSL services be similarly released from any requirement to connect to all ISPs or carry all services. In August 2005, they achieved this goal with the issuance of the FCC's Wireline DSL order.[25]

Many non-Bell VoIP and video/audio application providers also want to reach the Bells' subscribers, of course, and there is a tussle now over whether the Bells can either insist that these other application providers pay the Bells for the privilege of being accessed by end-users or subtly discriminate against non-Bell applications by degrading the quality of service experienced by users when using these other applications. The Bells have been extraordinarily active politically in trying to make sure that they have the power to control their networks, funds for the building of which may have been provided by their subscribers in the first place.[26] According to the Center for Responsive Politics, the Baby Bells have given more than $44 million since 1999 to federal candidates and parties (almost 60 percent to Republicans).[27]

In addition to consolidating consumers' bills, the Baby Bells are consolidating themselves. By the end of 2005, SBC (having purchased

24. National Cable & Telecommunications Association et al. v. Brand X Internet Services et al., 125 S. Ct. 2688, __U.S.___ (S. Ct. Jun. 27, 2005).

25. *In the Matters of Appropriate Framework for Broadband Access to the Internet over Wireline Facilities, Universal Service Obligations of Broadband Providers, Review of Regulatory Requirements for Incumbent LEC Broadband Telecommunications Services, Computer III Further Remand Proceedings: Bell Operating Company Provision of Enhanced Services; 1998 Biennial Regulatory Review – Review of Computer III and ONA Safeguards and Requirements, Conditional Petition of the Verizon Telephone Companies for Forbearance Under 47 U.S.C. § 160(c) with Regard to Broadband Services Provided Via Fiber to the Premises; Petition of the Verizon Telephone Companies for Declaratory Ruling or, Alternatively, for Interim Waiver with Regard to Broadband Services Provided Via Fiber to the Premises, Consumer Protection in the Broadband Era*, CC Docket No. 02-33, CC Docket No. 01-337, CC Docket Nos. 95-20, 98-10, WC Docket No. 04-242, WC Docket No. 05-271, Report and Order and Notice of Proposed Rulemaking, rel. Sept. 23, 2005 [DSL Order] (classifying wireline broadband Internet access service (DSL) as an information service under Communications Act).

26. *See generally* BRUCE KUSHNICK, THE $200 BILLION BROADBAND SCANDAL (2006).

27. New Jersey Record, *Untangling Telecom,* Aug. 7, 2005.

AT&T) dominated the western U.S. as the largest telecommunications company in the country, with about $110 billion in annual revenue, and Verizon (having purchased MCI) dominated the eastern portion of the country as the second largest telecom entity, with about $90 billion in annual revenue.[28]

The Bells' argument that they should have greater control over their networks has been given support by concerns about a related U.S. policy issue: broadband penetration. The Bells argue that unless they have greater control, and can monetize transmissions over "their" networks, they will have no incentive to continue building out broadband.[29] Whether because of the lack of competition for broadband provision or because of the peculiar physical characteristics of the wide-open U.S. landscape, or simply because of bad policy, the U.S. is falling behind in ensuring that its citizens have highspeed access to the internet. Studies by the Organization for Economic Cooperation and Development and the International Telecommunication Union have found that the U.S. is either 12th (OECD) or 16th (ITU) in the world in terms of the percentage of people having broadband access to the internet.[30] And broadband speeds in other countries are often four to five times higher than they are in the U.S. [31] The Bells argue that without having control over who has access to their networks, they will have no incentives to maintain or improve those networks and thus improve America's standing in the race to hook up citizens to the high-speed internet—and the Bells and the cable companies together control the market for broadband access in America.[32] So the Bells implicitly and explicitly suggest that the quid pro quo for improving the American broadband story should be control over their networks and the ability to block competing services unless they are compensated for carrying them.[33] In November 2005, SBC Chairman Edward Whitacre

28. USAToday, *supra* n.7.

29. *See* Susan P. Crawford, *Network Rules*, forthcoming 2006 (unpublished manuscript on file with author).

30. CQ Weekly, *supra* n.9; *see also* n.6, *supra*.

31. "Internet services in South Korea, Japan and Italy can transfer data at 8 to 10 megabits per second and are delivering sophisticated interactive games, online video and television programs to subscribers. In the United States, cable users can download information from the Internet at about 3 to 6 megabits per second; DSL users typically are limited to about 1.5 megabits per second." CQ Weekly, *supra* n.9; *see also* n.6, *supra*.

32. At the moment, broadband access is provided by just two kinds of actors in the U.S.: 95% of U.S. broadband subscribers are served by cable and telephone companies. Cable has more subscribers than the Baby Bells do, with 21.1 million subscribers to the Bells' 14.7 million. CQ Weekly, *supra* n.9.

33. Verso is already providing Skype blocking software to network providers. Ted Shelton,

made clear that SBC expected such control:

> [Q] How concerned are you about Internet upstarts like Google ( ), MSN, Vonage, and others?
>
> [A] How do you think they're going to get to customers? Through a broadband pipe. Cable companies have them. We have them. Now what they would like to do is use my pipes free, but I ain't going to let them do that because we have spent this capital and we have to have a return on it. So there's going to have to be some mechanism for these people who use these pipes to pay for the portion they're using. Why should they be allowed to use my pipes? The Internet can't be free in that sense, because we and the cable companies have made an investment and for a Google or Yahoo! () or Vonage or anybody to expect to use these pipes [for] free is nuts! [34]

Indeed, the larger goal of the Bells is to do away with the traditional telephone network, with all of its common carrier obligations and history of tariffing, altogether. Most traditional telephone lines in the U.S. will be replaced over the next five to ten years with DSL or fiber connections to the internet.[35] The digital, Internet Protocol[36] based systems of DSL and fiber are 30% to 60% cheaper to run than the old traditional telephone network. [37] So the traditional telephone companies are looking for ways to protect their markets against the depredations of their competitors as they move their businesses entirely onto the internet.

One key market-protection move is to pile destructive regulations on new competitors.[38] Several of the Bells have announced that they want to

Verso Appliance Lets Enterprises Block Skype, InformationWeek, Sept. 21, 2005.

34. BusinessWeek Online, Nov. 7, 2005. *See also* Arshad Mohammed, *SBC Chief Ignites Access Debate*, Washington Post, Nov. 4, 2005 (recounting reactions to Whitacre statements) ("Internet companies said Whitacre was stating what they have long feared -- that SBC and others may manage their networks to choke off access to Web sites or to target competing firms such as Vonage Holdings Corp. and Skype Technologies SA, which provide Internet-based phone services.")

35. Dave Burstein, DSL Prime, Nov. 25, 2005.

36. Internet Protocol (IP) is "the protocol used to route a data packet from its source to its destination via the Internet." Red Hat Documentation, Red Hat Glossary, at http://www.redhat.com/docs/glossary/.

37. DSL Prime, *supra* n.32..

38. Regulation is often used as a strategic barrier to entry. "An innocent entry barrier is

see that all VoIP providers meet the same "social policy" regulatory requirements that phone companies have had—including offering reliable emergency 911 service, submitting to the same federal wiretapping assistance guidelines to which traditional telephone companies are subject, contributing to the universal service fund, and paying access fees to connect to the traditional phone network.[39] The Bells themselves are content to comply with these regulations, because they have assumed in their planning processes that they will be subject to these continuing costs. But new entrants may not have planned for this kind of permission-based future, and are likely to be put out of business by the regulatory machinations of the incumbents. The VoIP providers had been working on voluntarily providing better, more informational, Internet Protocol-based E911 services, but the Commission chose instead to adopt a plan that appeared to be aimed at destroying them.

At the same time, a new class of regulatory capture players has emerged in the E911 and CALEA contexts: providers of outsourced compliance services to the Bells. A company called Intrado, which counts as its customers all of the Bells and most of the nation's wireless carriers, has over the past 25 years created a database of 206 million subscriber records, and now handles more than 80% of the existing emergency call infrastructure in the United States.[40] Intrado's footprint and pre-existing relationships with all of the companies involved who control the specialized hardware (called "selective routers") that must be used for

unintentionally erected as a side effect of innocent profit maximization. In contrast, a strategic entry barrier is purposely erected to reduce the possibility of entry." Steven Salop, Strategic Entry Deterrence, 69 Am. Econ. Rev. 335 (1979); s*ee* James B. Speta, *Deregulating Telecommunications in Internet Time*, 61 Wash. & Lee L. Rev. 1063, 1140 (2004) (examination of 1996 Act) (suggesting that "[r]egulation that burdens new entrants should be more suspect than regulation that burdens incumbents").

39. CQ Weekly, *supra* n.9. BellSouth CEO Duane Ackerman: "Congress must ensure that all the base-line social obligations placed on the communications business are equitably apportioned and supported by all competitors … regardless of the technology they choose to serve the public." Tech Law Journal, *BellSouth CEO Offers Recommendations for Next Telecom Act*, Dec. 14, 2005. John Langhauser, AT&T, before House Judiciary Cmte, at 77: "We agree with those who've said that providers of VoIP must meet important social policies." Verizon comments in IP NPRM, Dkt. No. 04-36, filed May 28, 2004, at 47-48: "[S]ome regulation of VoIP services is appropriate to effect important federal policy objectives. As Chairman Powell has recognized, "rules designed to ensure law enforcement access, universal service, disability access and emergency 911 service can and should be preserved in the new architecture." Verizon supports these objectives."

40. Russell Shaw, *Here's How Vonage-Verizon E-911 Will Work,* May 4, 2005, ZDNet; Robyn Weisman, *AT&T-Intrado E911 Deal Sign of Things To Come in VoIP World*, EWeek.com, Aug. 2, 2005. Stifel, Nicolaus Research Report (2003) (reporting 81% Intrado market share in wireless and wireline 911 provisioning; Intrado services almost all of the Baby Bells).

access to the nation's 911 system have made it possible for Intrado to provide a nationwide compliance product to VoIP companies.[41] Intrado *is* the company that under contracts with the Baby Bells runs most of the selective routers that are the gateways to the E911 system.[42] In effect, Intrado is now in a position to deliver all of the major VoIP providers' E911 calls itself.[43] Verizon,[44] SBC (now AT&T),[45] Vonage,[46] and Qwest[47] all use Intrado for their VoIP E911 service. Intrado is the ultimate middleman in this setting; anyone who wants to connect to E911 in this country needs to talk to Intrado first.

Another company, Level 3, serves as a key middleman for connection to the crucial selective routers. Level 3 provides myriad infrastructure and telecommunications services to many telephone and cable companies in both the United States and Europe.[48] It is certified as a "telecommunications carrier" in all 50 states—in effect, it has the status of a competitor to the Baby Bells—and claims that it has the network infrastructure to provide wholesale VoIP (and thus E911) services in areas covering approximately 69% of all U.S. households.[49] The Bells are required to permit Level 3 to interconnect with their E911 systems.

In the CALEA context, the key provider of outsourced compliance services is VeriSign, which presented itself to the FCC as able to provide outsourced "cost-effective CALEA support solutions" for all providers of

41. Intrado's customers include all of the Baby Bells (BellSouth, Qwest, SBC (now AT&T), and Verizon) and most of the wireless carriers in the U.S. Intrado Corporate Profile (last visited Dec. 10, 2005), http://www.intrado.com/main/company/history/intradocorporateprofile/.

42. See Letter from Mary Boyd, Vice President Government & External Affairs, Intrado, to Marlene Dortch, Secretary, FCC, WC Docket 04-36, Attach. at 1, 4-5 (filed Apr. 25, 2005).

43. Johanne Torres, *Intrado Interconnects Local Exchange Carriers*, TMCnet.com, Nov. 17, 2005; Robert Poe, *Intrado Lays the Groundwork for Nationwide VoIP E911,* Voip Magazine, Nov. 18, 2005; Charlotte Wolter, *Outsourced e911: Help is On the Way*, Xchange Mag, Aug. 1, 2005.

44. Verizon Compliance Report, Nov. 28, 2005, Dkt. No. 05-196.

45. Robyn Weisman, *AT&T-Intrado Deal Sign of Things to Come in VoIP World*, Aug. 2, 2005, Eweek.com.

46. Russell Shaw, Here's How Vonage-Verizon E-911 Will Work, May 4, 2005, ZDNet.

47. Mercator Capital VoIP Newsletter, Jan. 2005 (listing Qwest, along with Vonage, AT&T, and Verizon, as Intrado customer for E911 VoIP services).

48. Level3, The Level 3 Story, http://www.level3.com/576.html. Level3 is certified to connect to the selective routers around the country. *See* Level 3, E-911: Enhanced 911 for VoIP, http://www.level3.com/userimages/dotcom/pdf/Level_3_E-911_Fact_Sheet.pdf (Level 3 offers VoIP providers ability to provide full E911 service for approximately 60% of U.S. households with plans to support 70-80% later in 2005).

49. Press Release, Level 3 Selected by United Online to Enable VoIP Services, Dec. 15, 2005 (available at http://www.level3.com/press/6623.html).

broadband access and VoIP.[50] VeriSign suggested to the Commission that a "service bureau" approach to CALEA compliance would dramatically lower costs and simplify the task of law enforcement authorities, whose only interface would be with VeriSign rather than with all communications service providers.[51] VeriSign, which has announced publicly that its goal is to have all suppliers of communications services as its customers,[52] asked that the Commission's Notice of Proposed Rulemaking (NPRM) give "special consideration" to service bureau architectures in implementing CALEA.[53] The resulting CALEA NPRM did exactly that: it outlined VeriSign's proposal that the use of "trusted third parties" be recognized as fulfilling CALEA compliance obligations, and included an appendix sketching out VeriSign's proposed flow of data between entities.[54]

In addition to the incumbents pushing for telephony rules to be applied to the online world, and the outsourcing vendors pushing for standardized business opportunities, law enforcement and emergency services providers were anxious to receive familiar forms of data from new online companies and agitated for CALEA and E911 rules to apply to VoIP and other online applications.

The CALEA rulemaking discussed in this Article began with a petition filed on behalf of the Federal Bureau of Investigation, the Department of Justice, and the Drug Enforcement Administration asking

50. *In the Matter of United States Department of Justice, Federal Bureau of Investigation, and Drug Enforcement Administration Joint Petition for Rulemaking To Resolve Various Outstanding Issues Concerning the Implementation of the Communications Assistance to Law Enforcement Act*, RM No. 10865, Dkt. No. 04-295, Comments of VeriSign, Inc., Apr. 12, 2004.

51. Letter Anthony Rutkowski, VeriSign, to Marlene Dortch, Dkt. No. 04-295, Apr. 15, 2004 (attaching slides suggesting, among other things, that a service bureau approach to CALEA would facilitate subpoena process because online users could be easily identified). *See* EFF CALEA page entitled "the Perils of Wiretapping the Internet", available at http://www.eff.org/Privacy/Surveillance/CALEA/ ("Since compliance with surveillance requests is a significant cost for carriers, telecommunications companies have traditionally acted as a check on government power, lobbying against excessive proposals. Now, private entities that profit from surveillance will have an incentive to lobby for more government surveillance powers.")

52. Khali Henderson, *CALEA Compliance Goes Undercover,* Phone+, Jan. 2003, available at http://www.phoneplusmag.com/articles/311FEAT4.html ("The company [VeriSign] has the goal of supporting all suppliers, creating vendor neutral support for operators.") VeriSign, like Intrado, plans to migrate its pre-existing telecommunications carrier services to the online world.

53. Letter Anthony Rutkowski, VeriSign, to Marlene Dortch, Dkt. No. 04-295, Jul. 6, 2004.

54. *In the Matter of Communications Assistance for Law Enforcement Act and Broadband Access and Services,* ET Dkt. No. 04-295, RM-10865, Notice of Proposed Rulemaking and Declaratory Ruling, rel. Aug. 9, 2004 ("CALEA NPRM"), at ¶¶ 69-74 & App. C.

for clarification of the scope of CALEA.[55] The Joint Petition asked the FCC to declare that CALEA requires providers of broadband access services and "managed" VoIP services to design their facilities so as to make law enforcement wiretapping easier.[56] And the FCC, so far, has cooperated: In a notice of proposed rulemaking issued in August 2004, the FCC suggested that "facilities-based providers of any type of broadband Internet access service" and "'managed' Voice over Internet Protocol" services were subject to CALEA; more recently, the Commission has issued an order declaring that broadband access and "interconnected" VoIP services are covered.[57]

Ever since the 1994 enactment of CALEA, law enforcement, industry, and the FCC have been battling over what compliance with that statute requires of telecommunications carriers.[58] It is very likely that law enforcement authorities would like to replicate the call-identifying information that they have fought to obtain in the telephony world, and are interested in shifting the costs of sifting out that information to application

55. *In the Matter of United States Department of Justice, Federal Bureau of Investigation, and Drug Enforcement Administration, Joint Petition for Rulemaking to Resolve Various Outstanding Issues Concerning the Implementation of the Communications Assistance for Law Enforcement Act*, RM-10865, filed Mar. 10, 2004.

56. Supra n.__, at ___.

57. CALEA Order at __.

58. Industry groups came up with the first standard, which was known as the J-standard. Press Release, Telecommunications Industry Association, TIA and ATIS Publish Lawfully Authorized Electronic Surveillance Industry Standard (Dec. 5, 1997) at http://www.tiaonline.org/pubs/press_releases/1997/97-96.cfm. The FBI took strong exception to the J standard, and filed comments stating that the standard would have to be revised. See Communications Assistance for Law Enforcement Act, Comments of the Federal Bureau of Investigation Regarding Implementation of the Communications Assistance for Law Enforcement Act, CC Dkt. No. 97-213 (1997); Communications Assistance for Law Enforcement Act, Reply Comments of the Federal Bureau of Investigation Regarding Implementation of the Communications Assistance for Law Enforcement Act, CC Dkt. No. 97-213 (1998), available at http://www.askcalea.net/docs/980211.pdf. The FBI then issued a "punch list" of additional requirements it wanted to see incorporated in the J standard. Establishment of Technical Requirements and Standards for Telecommunications Carrier Assistance Capabilities under the Communications Assistance for Law Enforcement Act, Joint Petition for Expedited Rulemaking (1998) available at http://www.askcalea.net/docs/980327.pdf. The Joint Petition asked for: access to the communications of all parties in a conference call supported by the subscriber's service or facilities; access to all subject-initiated dialing and signaling activity; information indicating whether a party is connected to a multi-party call at any given time ("party hold," "party join," and "party drop" messages); notification of messages for in-band and out-of-band signaling; timely delivery of call-identifying information; automated reporting of surveillance status; delivery of all call-identifying information over call data channels; and a limited number of standardized delivery interfaces. These suggestions substantially raised the costs of compliance and led to litigation. United States Telecomm. Ass'n v. FCC, 227 F..3d 450 (D.C. Cir. 2000).

providers and their customers.[59]

In the E911 context, the role of the emergency services community is less obvious than the role of law enforcement in the CALEA proceeding. But it is clear that public safety officials from New York to Texas told the FCC that all VoIP applications should be immediately subject to E911 requirements.[60] And public officials told the FCC that they could not afford to have approaches to call centers made other than through the traditional selective router hardware route. For example, both the King County (Washington State) E911 Program and the City of New York told the FCC that they were very concerned about VoIP providers routing 911 calls to "administrative numbers" (numbers answered, if at all, by whatever clerk happens to be on duty) inside call center buildings – rather than through the selective router to emergency operators.[61] Many emergency services providers commented that they were concerned about losing funding for 911 services when phone subscribers switched to VoIP services. [62]

The combination of incumbent anxiety over future markets, third-party outsourced vendor interest in supplying compliance services, law enforcement desire for familiar forms of data, and public official anxiety over funding for emergency services (as well as over retaining orthodox approaches to emergency service provision) produced an irresistible incentive for the FCC to adopt E911 and CALEA rules affecting online services. The following Part describes these rules and outlines the

59. The CALEA NPRM sought further comment on how to define call-identifying information in packet technologies, and how much information is "reasonably available" to broadband access and VoIP providers.

60. *In the Matter of IP-Enabled Services*, WC Dkt. No. 04-36, Comments of King County E911 Program, May 27, 2004, at 2 ("The public expectation is that any device that can make voice phone calls can call 911. In addition, the public expectation is that full E911 service will be available on all telephone devices, including selective routing to the appropriate PSAP, and the provision of their call-back number and location information to the PSAP."; Comments of Eliot Spitzer, May 28, 2004, at 5 ("VoIP providers' products must allow their customers to access both traditional 911 and E911 systems.")

61. *In the Matter of IP-Enabled Services,* Comments of King County E911 Program, WC Dkt. No. 04-36, May 27, 2004, at 2; Letter Gino Menchini (Commissioner, City of New York Department of Information Technology and Telecommunications) to Marlene Dortch, WC Dkt. No. 04-36, Apr. 22, 2005; Letter from Gregory Ballentine, President, APCO International, to Kevin J. Martin, Chairman, FCC, WC Docket No 04-36 at 1 (filed Apr. 15, 2005) (APCO Apr. 15, 2005 Ex Parte Letter) (stating that while routing 911 calls to administrative numbers is "perhaps acceptable for some PSAPs, such an approach could endanger the public and disrupt already over-burdened PSAP operations" at others)..

62. E911 Order at ¶ 52 (citing comments).

controversies surrounding their implementation.

II. FCC INTERNET SOCIAL POLICIES

In March 2004, the FCC initiated a broad rulemaking proceeding suggesting that "social policies" from the world of telephony might be appropriate for the internet.[63] The FCC has begun its work in this area by focusing on two issues: availability of emergency 911 service and assistance to law enforcement. This Part describes, first, the differences between telephony and the internet, and, second, how the Commission proposes to implement these social policies with respect to online services.[64]

A. *Telephony v. Internet*

The fundamentals of telephony have not changed since its introduction. Early on, a pair of wires made up a circuit from the user to the operator and the operator would then complete the circuit between two users based on a caller's request. Later, the female operator was replaced by automatic switching systems and the analog circuits were replaced by digital channels. But the overall operation and concept of the telephone network (the PSTN, or "public switched telephone network") remains the same. When a user requests it, a digital circuit is opened between users for the duration of their call. This circuit carries the bits of information they want to send, and, whether or not the any user is saying anything, the circuit stays open until the call ends. Use of circuit switching therefore relies on intelligence—routing and processing decisions being made—

63. IP NPRM, *supra* n.___. *See* Susan P. Crawford, *Shortness of Vision*, 74 Fordham L.Rev. 695 (2005) (describing IP NPRM in global context of internet regulation).

64. Two other related initiatives, having to do with funding universal service and providing access to the disabled, are still under consideration and are not yet ripe enough to discuss. Chairman Martin has announced that imposing universal service funding obligations on internet services is one of his top priorities for 2006. Anne Broache, *FCC Chief Backs Net Phone Taxes*, CNET News.com, Dec. 14, 2005. A third internet-focused FCC initiative constraining the functioning of devices capable of retransmitting marked digital files online (the "broadcast flag" rule) was struck down by the D.C. Circuit in mid-2005. Amer. Lib. Ass'n v. FCC, No. 04-1037 (D.C. Cir. May 6, 2005). See Susan P. Crawford, *The Biology of the Broadcast Flag,* 25 Hastings COMM/ENT 603 (2003) (describing broadcast flag proceeding and jurisdictional weaknesses of FCC's claims of authority to regulate design of devices capable of processing TV signals (including PCs)).

residing at the center of the network. Indeed, a fundamental goal of telephony switches is to maintain control over circuits.[65] Every time a new service (like call waiting) is introduced, a tremendous amount of re-engineering of the network is required. For this reason, the scope of telephony services has not changed very much over the last fifty years. The idea of "someone in authority" standing between the user and the network, so prevalent in the early days of telephony, still exists.

This "someone in authority" notion is deeply connected to the presence of police and emergency assistance for telephone users. Indeed, from the very beginning of the history of telephony in the US, the essence of telephone service has been that it makes emergency help available from a central source. Telephones are there to watch over us in our sleep. For example, a major emphasis of early Bell advertising was the usefulness of the telephone in times of emergency. An ad from 1905 reads: "The modern woman finds emergencies robbed of their terror by the telephone. She knows she can summon her physician, or if need be, call the police or fire department in less time than it ordinarily takes to ring for a servant."[66] A 1910 Bell-funded telephone tract put the matter this way:

> But it is in a dangerous crisis, when safety seems to hang upon a second, that the telephone is at its best. It is the instrument of emergencies, a sort of ubiquitous watchman. When the girl operator in the exchange hears a cry for help -- ``Quick! The hospital!" ``The fire department!" ``The police!" she seldom waits to hear the number. She knows it. She is trained to save half-seconds. And it is at such moments, if ever, that the users of a telephone can appreciate its insurance value. No doubt, if a King Richard III were worsted on a modern battlefield, his instinctive cry would be, ``My Kingdom for a telephone!" . . . When a small child is lost, or a convict has escaped from prison, or the forest is on fire, or some menace from the weather is at hand, the telephone bells clang out the news, just as the nerves jangle the bells of pain when the body is in danger. In one tragic case, the operator in Folsom, New Mexico, refused to quit her post until she had warned her people of

65. *See generally* Susan Landau, *National Security On the Line* 18 (2005) (discussing differences between circuit-switched and packet-switched networks) (citing Andre Girard, *Routing and Dinensioning in Circuit-Switched Networks* (1999) at 431).

66. FISCHER, AMERICA CALLING, *supra* note ___, at 140.

> a flood that had broken loose in the hills above the village. Because of her courage, nearly all were saved, though she herself was drowned at the switchboard. Her name -- Mrs. S. J. Rooke -- deserves to be remembered.[67]

A Bell ad from the 1910s features a drawing of a maiden in a nightdress clutching her throat and looking anxiously out the window. The ad copy reads: "When You Need a Neighbor – or a doctor or assistance of any sort at any time, a reliable telephone is a friend in need. It is a time-saver when time is most valuable; often a life-saver in illness – a property-saver in fire or theft..But you cannot get the full service, value and benefit of a telephone unless you have a reliable telephone – buy and use only Standard "Bell" Apparatus and Equipment."[68] An ad from the 1920s reads: "my heart stood still . . . I heard stealthy voices . . . someone tinkering with a lock . . . a muffled footstep . . . saw a shadow flit by my window . . . I reached over to the stand by the bedside and seized – no, not a revolver – a telephone."[69] An ad from the 1930s shows a picture of a little blond girl, arms innocently flung out in sleep. The ad reads: "Sleep Soundly, Little Lady..."Mother and Daddy are near and the telephone is always close by. It doesn't go to sleep. All through the night it stands guard over you and millions of other little girls and boys."[70] Two other 1930s ads have the same theme. One features a little boy in bed looking apprehensively at his mother, and reads: "Your Cheapest Servant Protects Your Dearest Possessions. Sickness. . . . it is economy to have a means to reach your doctor quickly. Fire? .. . . a few minutes delay will cause great damage. Accident or thieves? . . . nothing will bring you help as quickly as the telephone! Really, how much value can you place on something that makes life easier and safer?"[71] The other is directed to farmers, and shows a young girl at the phone while a prowler lurks outside her window: "Your Home Deserves Protection. A telephone on a farm is the greatest obstacle to rural thieves..." [72] An ad from the 1940s says that telephone service is a bargain because it is "Advantageous to you because it saves time, steps, and trouble. Stands guard over the security of your home. ..."[73] Telephones are vigilant, centrally-controlled, located in an identifiable

67. CASSON, HISTORY OF THE TELEPHONE, *supra* note ___, at 211-213. Of course, that was not really her name. That was (mostly) her husband's name. But I digress.

68. Advertisement on file with author.

69. FISCHER, AMERICA CALLING, *supra* note ___, at 68.

70. Advertisement on file with author.

71. FISCHER, AMERICA CALLING, *supra* note ___, at 118.

72. FISCHER, AMERICA CALLING, *supra* note ___, at 119.

73. Advertisement on file with author.

terrestrial place, and set up with services that the telephone company believes (or the government believes) are good ideas.

By contrast, the internet has none of these characteristics. There is no one in authority between the user and the network, there is no central control, there is no necessary terrestrial connection to particular internet uses, there is no advertising for the internet touting its connection to emergency services, and anyone can begin a new service that is available around the world without asking permission from anyone else. You can make a VoIP call from a hotel room in London using a New York area code number, and "be" for all purposes (except physical purposes) in New York.

The internet is not a telephony network in part because it is "packet switched" rather than "circuit switched," and in part because internet packets have no guarantees of service. The Internet Protocol (or IP) can be understood as a language that allows the division of all communications into small packets that are then individually routed, one hop at a time, to their destination—without any router knowing more than where the next hop is. Because internet traffic has been packetized, there is no need for it to occupy a circuit for the full duration of an exchange. Instead, you can use the circuit just for the brief interval needed to transmit the packet. And because each packet has a unique source and destination address embedded in its header, simultaneous conversations can coexist on the same circuit without interfering with one another, and without anyone having to be in charge of the routing of these conversations.[74]

The telephone network was built for a single purpose: voice telephony. By contrast, the Internet Protocol provides a simple, common interface for all kinds of networked applications to run over all kinds of physical networks.[75] Thus, fiber-optic infrastructure or wireless connections afford or provide a way for any networked application to be transmitted, and the Internet Protocol affords or provides a predictable, well-defined interface for these transport mechanisms to work with applications.[76]

74. *See generally* HowStuffWorks, *How Internet Infrastructure Works*, available at http://computer.howstuffworks.com/internet-infrastructure.htm.

75. *See* Lawrence B. Solum & Minn Chung, *The Layers Principle: Internet Architecture and the Law*, 79 NOTRE DAME L. REV. 815 , 822 (2004) (noting that layers are key architectural element of the internet and drive normative conclusions about internet regulation).

76. *Id*. The layers concept has recently become a suggested model for regulatory

Implementation of the Internet Protocol provides the means to allow the end-to-end principle first articulated in an important paper by Jerome Saltzer, David Reed, and David Clark in 1984 to be implemented.[77] The end-to-end principle suggests that suggests that communications, that is, the information contained in the IP packet's payload, ideally should not be filtered or changed or operated on by the network itself, but only by the edges, at the level of applications that individuals set up and manipulate.[78] This end-to-end principle, like the Internet Protocol, 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.

Where a central telephone provider must provide enhanced functionalities at a physical termination point, IP network design is highly decentralized, allowing substantial innovation to occur at the edges of the network. Internet routers have not (to date) been designed to maintain control or accountability over circuits, or even remember anything about the packets that pass through them. Instead, internet routers are designed only to forward packets one more step toward their destinations, and have no necessary connection to geography. Because of its protocols and layers, the internet allows any application to be used on any network and in any geographical location.

The protocols of the internet have made innovation easy. Having to ask permission to introduce a new service, at any layer, is enormously destructive to the internet model that has brought such great benefits to the U.S. economy. There are better ways to meet law enforcement's needs for data that do not involve the FBI in internet application design, and there are better ways to provide emergency services that do not involve forcing new applications to connect to ancient legacy hardware installations.

By contrast, the telephone network is completely geographically dependent and has been designed to carry a single application. In

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, *A Horizontal Leap Forward: Formulating a New Communications Public Policy Framework Based on the Network Layers Model*, 56 FED. COMM. L.J. 587 (2004).

77. Jerome H. Saltzer, David. P. Reed, & David. D. Clark, *End-to-End Arguments in System Design*, 2 ACM TRANSACTIONS ON COMPUTER SYSTEMS 277 (1984).

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

telephone networks, that application (phone service) and the physical connection to the network itself are inextricably intertwined. This geographic fixity has made 911 service and wiretapping possible on telephone networks.

B. E911

There are likely many potential technologies, including location-aware services, that will benefit society enormously but may never come into being because of the E911 Order. First, there are substantial technical standard-setting activities underway that may be truncated because of the FCC's approach.[79] Second, starting in 2003, the National Emergency Number Association (NENA), the group that coordinates Public Safety Answering Point (PSAP—the call centers used for 911 services, described in the following section) efforts, began working with online VoIP companies to develop more innovative solutions for E911 services.[80] A Voice on the Net (VON)/NENA 911 working group was established in 2004 to implement the NENA efforts. And several VoIP providers began deploying interim 911 services—something that took wireless carriers sixteen years to do. The VON/NENA efforts resulted in plans to roll out an IP-based E911 service offering which would deliver location information and callback numbers to PSAPs automatically in real time via the internet (rather than connecting through the traditional telephone system). As of February 2005, the plan was for these services to include enhanced digital capabilities:

79. The IETF is working on modifications to the Dynamic Host Control Protocol to allow a device to be assigned location information by a network when the device first connects to that network. *See, e,g,,* RFC 3825, "Dynamic Host Configuration Protocol Option for Coordinate-based Location Configuration Information," published July 2004, available at http://www.ietf.org/rfc/rfc3825.txt; H.Schulzrinne, Internet Draft, "Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Option for Civic Addresses Configuration Information," published May 2005, available at http://www.ietf.org/internet-drafts/draft-ietf-geopriv-dhcp-civil-06.txt (work in progress) (both cited by the Center for Democracy and Technology in comments on the E911 Order). There are proposals for voluntarily-provided emergency services based on instant messaging and other IP-based services. *See, e.g*., H. Schulzrinne, *Emergency Services URI for the Session Initiation Protocol*, published Feb. 2004, *available at* http://www.ietf.org/proceedings/04aug/I-D/draft-ietf-sipping-sos-00.txt (work in progress)

80. December 2003 NENA agreement with 8 X 8, AT&T Consumer Services, Broadsoft, Dialpad, ITXC (now TeleGlobe), Level 3, PointOne, Pulver.com, Vonage, and Webley, referenced in Voice on the Net Coalition, *9-1-1: Answering the Call for 9-1-1 Emergency Services in an Internet World, a 9-1-1 Primer and Progress Report on the VON/NENA Agreement*, Jan. 12, 2005, at 2, *available at* http://www.von.org/usr_files/911%20VON%20White%20Paper%201-12-05%20final.pdf.

> By upgrading to Internet Protocol (IP) based equipment, 9-1-1 calls could be accompanied by much more information, such as a callers' medical records, medical status, language preference, or maps of commercial buildings. With today's system, there is no way for end users to automatically inform emergency technicians that someone has Alzheimer's, or for a PSAP to receive photo or video images. In the future, VoIP 9-1-1 calls may be able to support not only voice but a variety of data and video features/functions.[81]

Several companies put aside work on more robust emergency response efforts to devote their resources to complying with the FCC's approach in the E911 Order.[82] And because the FCC E911 Order was implemented before the public safety community finalized what had become known as the NENA "I2" standard,[83] major providers (including Intrado) implemented versions of E911 services that comply with the E911 Order but are noncompliant with the I2 standard—thus creating a continuing patchwork of E911 services.[84]

Obviously, because the E911 Order requires all VoIP 911 calls to go through the selective router, it will not allow a 911 call to go through an Internet Protocol router to any call center. It therefore prevents any IP-based emergency network (together with the host of advances such a network can deliver) from coming into being. The FCC's June 2005 E911 Order cut off further development of these IP-based E911 services, and sent companies scrambling to figure out how to connect with a legacy, centrally-switched, telephony-based 911 system. Although commentators

81. *Id*. Former FCC Chairman Michael Powell applauded these efforts: "The 9-1-1 system is vital in our country, but it has limited functionally. In most systems, it primarily identifies the location from which the call was made. But an Internet voice system can do more. It can make it easier to pinpoint the specific location of the caller in a large building. It might also hail your doctor, and send a text or Instant Message alert to your spouse." .

82. The Department of Commerce had encouraged the development of a post 9/11 reverse 911 emergency broadcast system, and the city of Herndon, Virginia had developed an Amber Alert system over Cisco VoIP phones. Rather than continuing with work on breakthrough advances like these, companies put aside these efforts to focus on compliance. Email Jonathan Askin, pulver.com, to the author, Feb. 12, 2006.

83. *See generally* NENA, *Interim VoIP Architecture for Enhanced 9-1-1 Services (I2),* white paper dated Aug. 5, 2005 (after the May/June 2005 adoption of the E911 Order). (FCC Orders are announced and adopted a month or more before the text of the Order is released.)

84. Email Jonathan Askin, pulver.com, to the author, Feb. 12, 2006.

had suggested that VoIP not be burdened with connecting to the legacy emergency system (noting, for example, that "[t]oday's emergency access network reflects the hierarchical nature of the incumbent local exchange network"),[85] and had pointed the Commission to enhanced capabilities that IP-based emergency services communications could include, the Commission ignored all of this and plunged forward (or backward) to tie emergency services to the existing legacy infrastructure.[86] Many new VoIP entrants may be driven out of business by these requirements.

i. Background

In April 2003, a Colorado mother watched her infant son die while she was switched from one 911 dispatcher to another.[87] She blamed Comcast, her digital phone provider, for failing to record her address accurately.[88] In early 2005, a Houston teenager's parents were shot during a robbery.[89] The teenager used a Vonage VoIP phone to call 911, and allegedly had trouble reaching a 911 dispatcher.[90] Similarly, in March 2005 a mother in Deltona, Florida tried to use her Vonage phone to dial 911 when her daughter stopped breathing, but was unable to get through.[91] Her daughter subsequently died. The Attorneys General of three states, Texas, Michigan, and Connecticut, all sued Vonage, claiming that users had been deceived as to Vonage's 911 capabilities.[92]

Vonage called itself "The Broadband Phone Company," but it

85. *In the Matter of IP Enabled Services*, WC Dkt. No. 04-36 and WC Dkt. No. 03-266, Comments of Level 3 Communications, at 37, filed May 28, 2004.

86. *See, e.g.,* Hatfield Report at 41. Dale N. Hatfield, A Report on Technical and Operational Issues Impacting The Provision of Wireless Enhanced 911 Services at 41 (2002), available at http://gullfoss2.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=6513296239. An IP-enabled emergency service system would enable "a caller to send a picture of a vehicle involved in a hit-and-run accident along with a voice message." Id. IP-enabled emergency services would allow deaf users to contact others.

87. Chris Vanderveen, *Mom Blames Phone Company Mix-Up for Death of Son*, 9news.com, Sept. 30, 2004.

88. Chris Vanderveen, *Mom Blames Phone Company Mix-Up for Death of Son*, 9news.com, Sept. 30, 2004.

89. Ben Charny, *Deadly Delay on Vonage 911?*, News.com, May 9, 2005.

90. Ben Charny, *Deadly Delay on Vonage 911?*, News.com, May 9, 2005.

91. Ben Charny, *Deadly Delay on Vonage 911?*, News.com, May 9, 2005.

92. Eric Hellweg, *VoIP's Call for Help*, MIT Technology Review, Mar. 25, 2005 (Texas); Ted Stevenson, *State To Target Vonage 911 Services*, Internetnews.com, May 2, 2005 (Michigan); Preston Gralla, *Connecticut Sues Vonage Over Emergency 911*, Networkingpipeline.com, May 5, 2005 (Connecticut).

apparently was not providing adequate 911 connectivity. At an open FCC meeting on May 19, 2005, people involved in these Vonage incidents– including Cheryl Waller of Florida, the mother of the baby girl who died– testified to the effect that their expectation had been that they would be able to reach 911 operators just as with an "ordinary" phone.[93] Waller's testimony in particular was extraordinarily troubling:

> In a hushed hearing room at the FCC headquarters last May, Cheryl Waller choked back tears as she recounted the death of her three-month-old daughter. At 6:35 p.m. on Mar. 24, the baby stopped breathing. The frantic mother dialed 911 several times but got only a voice recording. Finally, a neighbor reached a 911 operator -- but by the time medics arrived, it was too late. The infant was pronounced dead at 6:51 p.m.
>
> Waller . . . urged the Federal Communications Commission to pass Chairman Kevin J. Martin's proposal to require Internet carriers to tighten up their emergency services within 120 days -- ``seven days longer than my daughter lived," said Waller, dissolving into tears.[94]

It seemed so easy – why *not* require the "The Broadband Phone Company" and other VoIP providers to make 911 service available to their subscribers, particularly when people could die if such service was not available? On the same day that Waller appeared before them, the FCC Commissioners voted 4-0 to adopt the E911 Order.[95]

93. No one I spoke to at the FCC could recall any past Commission meeting featuring a "victims panel" like the one that was convened for the E911 session. It was an unprecedented piece of theater. Note that all of the narratives presented had to do with problems with Vonage services. There has been speculation that the entire E911 proceeding was aimed directly at Vonage by Chairman Martin. Vonage's somewhat bombastic CEO, Jeffrey Citron, had supported Michael Gallagher—and not Kevin Martin—for the post of FCC Chairman. Vonage was a favorite company of Martin's predecessor, Michael Powell, with whom Martin had had many political clashes. (Powell supported Gallagher over Martin as well.) The E911 proceeding can be seen as vengeance for all of these activities. The role of third-party outsourced service providers in the E911 context was also deeply significant to the Commission's actions, however, and so I am focusing on this slightly less vendetta-like capture reason for the adoption of the E911 Order.

94. Catherine Yang, *Storm Warnings for Kevin Martin: The New FCC Chairman is About To Confront Issues that Divide Business*, BusinessWeek, Oct. 31, 2005.

95. FCC Press Release, *Commission Requires Interconnected VoIP Providers To Provide Enhanced 911 Service: Order Ensures VoIP Customers Have Access to Emergency Services*, May 19, 2005 (Washington, D.C.).

Given the differences between the way that traditional telephone networks work and the way the internet works, the E911 Order was a very dramatic piece of administrative activity. Briefly,[96] landline (traditional, non-wireless telephone) 911 works in this country because we have established a network of 6000 "Public Service Answering Points," or PSAPs, whose staffs field 911 calls. Specialized routing within the telephone network, using centrally-programmed switches, ensures that a 911 call goes to the right PSAP. But, in the beginning, basic landline 911 calls did not arrive accompanied by location information or a callback number. This meant that the PSAP operator had no way to call the complaining person back or send an ambulance to the right destination, unless the caller was able to describe his or her whereabouts and provide a number (something many people in an emergency are unable to do).

Using signals that automatically made analog queries to a billing database, PSAPs and local telephone companies were able to obtain the calling number. (This is what software developers would call a "kludge," or inelegant work-around allowing a desired result.) A separate kludge was set up to allow PSAP equipment to automatically query an "Automatic Location Identification" (ALI) database over a separate data circuit (separate from the call itself), telling the ALI the phone number that is calling in. The ALI then returns location information to the PSAP.

In time, local telephone companies were able to program "selective routers" (hardware) to query these databases and provide both a callback number and location information to a PSAP at the same time that the 911 call was coming in. Thus enhanced 911 (or E911—911 that includes location information and a call-back number) came into being thirty years ago, based not on digital signaling but on centralized router programming by phone companies. This was possible for telephone companies that had knowledge of the subscriber's location for billing purposes; indeed, this 1970s E911 system was dependent on using numbers that closely tied to both subscriber location and existing physical network switches.

Wireless carriers do not have selective routers of their own. They need the permission and active cooperation of the carriers who control

96. As was the FCC itself, I am indebted to Dale N. Hatfield and his report, *A Report on Technical and Operational Issues Impacting the Provision of Wireless Enhanced 911 Services*, *available at* http://gullfoss2.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=6513296239, prepared for the FCC in late 2002 [hereinafter Hatfield Report], for the description of 911 impossibilities that follows.

these selective routers to connect to them. Without these connections the wireless industry cannot provide accurate information to existing PSAPs. For this reason, the FCC and the wireless industry have been working since 1993 on wireless E911 arrangements, with countless extension and waiver requests being filed by the wireless companies.[97] The details of these negotiations are not important, but the bottom line is that given the kludges and legacy systems in place for landline PSAPs, as well as the absence of incentives for telephone companies to allow wireless companies to interconnect with their selective routers, it has proven extremely difficult to have E911 services implemented for wireless subscribers. Because 911 continues to be based on a 1970s legacy system, it has taken more than ten years for nomadic cellphones to have reliable 911 access.[98] Cell phone operators use tower location and triangulation to make location information availabled for 911 purposes (information that is not available to mobile VoIP providers).

Despite the history of slow and difficult implementation of 911 on the wireless side, FCC Chairman Kevin J. Martin must have felt he had to act quickly to address the searing press coverage of deaths caused (arguably) by inadequate VoIP 911 service. On May 19, 2005 after Cheryl Waller gave her testimony about the death of her daughter and the Commission adopted the E911 Order, Chairman Martin said: "Today's action seeks to remedy a very serious problem -- one quite literally of life or death for the millions of customers that subscribe to VoIP service as a substitute for traditional phone service,"[99]

In the E911 Order, the Commission mandated that "interconnected VoIP" providers be able to route all 911 calls (accompanied by a call-back number and the caller's location) through the traditional telephone 911 network to appropriate local emergency authorities by November 28, 2005.[100] The Commission defined "interconnected VoIP" as those services that (1) allowed for real-time, two-way voice communications, (2) required a broadband connection, (3) required end-user equipment to process and receive Internet Protocol packets, and (4) allowed users to *both* receive calls from traditional telephone networks *and* make calls to telephone

97. *See* Kelly Carroll, *One Fine E911 Mess*, TelephonyOnline, Aug. 20, 2001 (noting delays and extension requests).

98. According to the CEO of VoIP provider Nuvio, "The cellular industry has been grappling with these [E911 implementation issues] for a dozen years." Jon Van, *VoIP Provider Files Suit, Seeks Clarity from FCC*, Chicago Tribune, Aug. 16, 2005.

99. Martin statement accompanying E911 Order.

100. E911 Order.

numbers.[101] Thus, a free online voice service that made it possible for users to "call" traditional telephone numbers and receive "calls" from the network must find ways to get "location" and "callback" information to a "local" emergency center through a centrally-located and customized piece of hardware—the selective router—controlled, for the most part, by Intrado.[102]

"Interconnected VoIP" providers were also directed to find ways to obtain updated information as to the physical locations of their subscribers, and were told that they had to instruct their customers immediately (and obtain affirmative acknowledgements from subscribers that they had received these instructions) as to the extent of 911 service provided to them.[103] Providers of these "interconnected VoIP" services were ordered to find ways to make 911 services available to their subscribers, and told that connecting to the existing 911 legacy structure was a condition of their being permitted to provide services at all.[104] The Commission noted that third-party providers of outsourced services (including, prominently, Intrado) were available to assist "interconnected VoIP" providers with connections to the traditional telephone 911 system – because these providers had been certified as telecommunications carriers.[105] The Commission also said it would not shield "interconnected VoIP" providers from liability under state laws for mistakes occurring in connection with provision of emergency services. Telephony providers, both wired and wireless, do have such liability protections by statute.[106]

101. E911 Order at ¶ 24. Catherine Yang, *Storm Warnings for Kevin Martin: The New FCC Chairman is About To Confront Issues that Divide Business*, BusinessWeek, Oct. 31, 2005.

102. As the Commission notes, 911 systems "usually are based on a 25-year-old architecture and implemented with legacy components that place significant limitations on the functions that can be performed over the network." *Id.,* E911 NPRM, ¶ 59, at 34.

103. E911 Order at ¶ ¶ 45-49.

104. E911 Order at ¶ 47 ("Thus, interconnected VoIP providers must, as a condition of providing that service to a consumer, provide that consumer with E911 service as outlined in [this Order].")

105. E911 Order at ¶ 38. The Baby Bells are required to provide access to 911 databases and interconnection to 911 facilities to all telecommunications carriers, pursuant to 47 U.S.C. §§ 251(a) and (c) and § 271(c)(2)(B)(vii) of the Telecommunications Act.

106. *E.g.*, Wireless Communications and Public Safety Act of 1999 Sec. 4(a), Pub. L. No. 106-81, 113 Stat. 1286 (1999) (providing wireless carriers, and their officers, directors, employees, vendors and agents the same immunity or protection from liability as local exchange companies enjoy in the same jurisdiction). Both liability protection and mandated access to selective routers are being addressed by draft bills now pending in Congress. Communications Daily, Nov. 3, 2005.

ii. Implementation Difficulties

Making E911 services available to consumers within four months was impossible to do for most VoIP companies.[107] As discussed above, the existing 911 infrastructure in the U.S. is extremely antiquated, to the point where even wireless companies have had great difficulty implementing 911. The E911 Order gives "interconnected VoIP" providers no new rights that will help them comply, and does not obligate local telephone companies to allow them to connect to the essential "selective routers" owned by these telephone companies.[108] Thus, VoIP service providers have no right to access selective routers, and have to wait for the Bells to (slowly) give them permission to connect. The E911 Order did not set rates or otherwise control what the essential facility provider—the incumbent local telephone company—could do to hold up a VoIP provider seeking access to the special emergency communications equipment whose use the E911 Order mandated. (FCC has also sought comment on whether these 911 obligations should apply to entities other than "interconnected VoIP" providers, and this broader ranger of entities will likely have even more difficulty with the requirements of the E911 Order.)[109]

The complexities of nomadic VoIP services (usable from any net connection anywhere in the world, using any area code, over any form of transport) make connection to the legacy E911 system difficult. Thus, online voice providers will need to persuade the Bells to give them access to the necessary facilities through intermediaries at a sensible cost, and load up routers and databases with the right information, without any protection

107. *See FCC's Deadline To Make VoIP Services E-911 Capable Will Be Difficult To Meet*, WARREN'S WASHINGTON INTERNET DAILY, Jun. 9, 2005; Charlotte Wolter, *Vonage CEO Citron: No One Can Meet FCC 911 Deadline*, NEW TELEPHONY, Jun. 14, 2005.

108. *See FCC Adopts Order Expanding E911 Regulation To Include Some VOIP Service Providers,* TECH LAW JOURNAL, May 20, 2005, *available at* http://www.techlawjournal.com/alert/2005/05/20.asp.

109. E911 Order at ¶ 58. Vonage, in particular, bitterly complained to the FCC that although BellSouth and SBC were giving the appearance of cooperating in granting access to their selective routers to Vonage, they were in fact making such connection difficult. *See*, *e.g.,* Letter Jeffrey Citron of Vonage to Bill Smith, CTO of BellSouth, attached to Vonage May 10, 2005 ex parte filing.("I write to seek your clarification that BellSouth will make available all elements necessary to allow Vonage and BellSouth to implement a solution that will allow for the extending the benefits of E911 to nomadic VoIP consumers"); Letter Vonage to Marlene Dortch, May 10, 2005 ("contrary to the public pronouncements of several RBOCs, many of the proposed solutions are limited to delivery of 911 to fixed location end users with geographically valid telephone numbers") (attaching letter from SBC); Letter Vonage to Marlene Dortch, May 13, 2005 ("SBC's recently announced VoIP 'solution' is inadequate and does not fully support nomadic VoIP providers. . . Vonage often has difficulty provisioning selective router trunking because of limitations in carrier interconnection agreements.").

from liability if they make mistakes. Compliance may be sufficiently expensive to make it no longer worthwhile for some VoIP providers to stay in business.[110]

In the E911 Order, the FCC firmly told providers of "interconnected VoIP" operators that if they did not comply with the Order by November 28, 2005, they would be forced to stop offering services to customers.[111] In October 2005, Nuvio (a VoIP company) sued the FCC seeking a stay of the E911 Order's requirements.[112] Then, in November 2005, prompted by Nuvio's and other industry complaints,[113] the FCC backed down. VoIP providers were told that if they did not comply with the E911 Order as of November 28, 2005, the Commission "would expect that such providers will discontinue marketing VoIP service, and accepting new customers for their service" in areas where E911 services were not available.[114] The Commission "strongly encourage[d]" VoIP providers to adopt the E911 compliance plans that had been filed by AT&T and Verizon when they merged with SBC and MCI, respectively (plans that had been exacted by the Commission as a condition of the mergers), including commitments not to accept new customers in areas where E911 service was not available.[115]

110. Indeed, pulver.com has "chosen not to offer a PSTN-connected VoIP service in the US because of the FCC's backward-looking, anti-innovative rules on E-911 and CALEA." Email Jonathan Askin of pulver.com to the author, Dec. 20, 2005.

111. *See* 47 C.F.R. § 9.5(e).

112. Nuvio E911 Requirements for IP Enabled Service Providers, WC Docket No 05-196, [Nuvio, et al.] Motion for Partial Stay, at 5-9 (filed Oct. 24, 2005) (citations omitted).

113. E.g., VON Coalition November 2005 ex parte filing, reporting survey of independent VoIP providers (nearly half of those surveyed said they would have to cut off customers because they could not meet the Commission's Nov. 28 deadline).

114. FCC Public Notice, Enforcement Bureau Outlines Requirements of November 28, 2005 Interconnected Voice Over Internet Protocol 911 Compliance Letters, WC Docket No. 04-36, WC Docket No. 05-196, DA 05-2945 (rel. Nov. 7, 2005).

115. Public Notice, *Enforcement Bureau Provides Guidance to Interconnected Voice Over Internet Protocol Service Providers Concerning the July 29, 2005 Subscriber Notification Deadlines,* WC Docket 04-346, WC Docket 05-196, DA 05-2085 (rel. Nov. 7, 2005) at 2. The Verizon and AT&T plans included a wildly kludge-y way of updating consumer location information: "By November 28, Verizon expects to have a capability to detect when a customer's VoiceWing telephone adapter is disconnected from the network. If we detect that the customer's adapter has been disconnected, we will suspend the customer's service, with the exception of 911 calls and calls to customer service. At the same time, we will send the customer an e-mail and post a message to the customer's Personal Account Manager asking the customer to confirm his or her existing Registered Location, or register a new location. While in suspend status, if the customer attempts to make any calls, other than 911 calls or calls to customer service, before he or she confirms or registers a new location, Verizon will intercept the call and play an announcement that will inform the customer of the service suspension and transfer the customer to a customer service representative for assistance. If the customer confirms to the service representative that the customer's Registered Location has not changed, full service will be

The clear implication to be drawn from this "strong encouragement" was that VoIP providers who did not file equivalent compliance plans by November 28, 2005 (the date by which compliance with the E911 Order was required) would be viewed as being candidates for enforcement actions. Neither wireline nor wireless providers have ever been required to obtain acknowledgements from their subscribers of the limitations of their 911 services, to disconnect subscribers because of these limitations, or to limit their marketing efforts—even though it has taken wireless providers more than a decade to get E911 services working.

Most VoIP providers missed the November 28 deadline,[116] and some, including Vonage, continued to market services to customers even though E911 service was not available.[117] Let us say you are sitting in London using a U.S. online voice service with a Rhode Island number, and you are speaking to a friend in Singapore. Let us assume you get into some kind of trouble. How is the online voice application supposed to know who to tell, and what to tell them to do? The answer, for the moment, is that the online voice application is supposed to make arrangements through local phone companies and with all selective routers (which are in turn connected to their relevant PSAPs) to provide databases of location information and callback numbers—and that this location information is supposed to be provided and updated by the subscriber, even if the subscriber is going 90 miles per hour down a Montana freeway. (The FCC appears to be planning to require any VoIP-capable device (including PCs) to be able by June 2006 to *automatically* declare its location.)[118]

restored by Verizon. If the customer indicates that he or she has moved from the existing Registered Location, service will remain suspended unless and until the customer registers a new address in an area where Verizon can provide 911 service. If the customer fails to choose either option (for example by hanging up), service will remain suspended . . . As a result, the customer will be required to register a new address when the service is used nomadically." Verizon Ex Parte filing in WC Docket 04-36, WC Docket 05-196, Oct. 21, 2005.

116. Geoff Duncan, *VoIP Providers Largely Miss E911 Deadline,* DesignTechnica.com, Nov. 30, 2005.

117. Roy Mark, *Vonage Markets On Despite FCC E911 Order*, InternetNews, Nov. 29, 2005. Vonage sought a waiver of the FCC rule, stating that it had been able to extend E911 service to only 26% of its subscribers. More than a dozen other VoIP companies also sought waivers. As noted above, supra n.__, it is difficult for VoIP providers to limit who sees their online advertisements. Additionally, this marketing requirement seems to plunge the FCC deeply into advertising regulation—territory thought to be within the purview of the Federal Trade Commission. If the FTC does get involved, it might require bold letter warnings: "You are not buying a telephone service. If you want telephone services, go somewhere else."

118. In Paragraph 57 of the E911 NPRM, the Commission asks whether it should "require all terminal adapters or other equipment used in the provision of interconnected VoIP service sold as of June 1, 2006 to be capable of providing location information automatically, whether embedded in other equipment or sold to customers as a separate device?" This suggestion that eventually all

And what exactly is a "VoIP provider"? The internet is indifferent to the nature of the applications that it carries. In turn, to each application one bit looks just like another.[119] So, for example, instant messaging platforms that include many straight data tools (text, maps, collective picture drawing, file sharing) can also easily include voice applications—which are also straight data tools.[120] The instant messaging (IM) user can talk to others to his or her heart's content. Are IM providers "VoIP providers"? At the moment, the answer from the FCC is "Not necessarily," because most of these applications do not make it possible to both send data to particular phone numbers and receive data "at" a particular phone number (and thus are not "interconnected" VoIP providers).[121] But in time more of these applications may have this capability, or the FCC may broaden the scope of its rule to include them.[122] The FCC is already signalling that its definition of "interconnected VoIP" will broaden to include VoIP applications that are "capable of" connection to traditional telephone networks.[123]

More fundamentally, there is no magic distinction between "voice" data and any other kind of data. Voice when digitized looks and acts just

VoIP-capable applications and devices (including PCs) should be automatically reporting their precise locations should raise substantial privacy concerns and worries about technical mandates. *See* Part IV, infra.

119. 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.

120. *See* INFORMATIONWEEK, May 16, 2005: "Spending by U.S. companies and public-sector organizations on voice-over-IP systems will grow to $903 million this year, up from $686 million in 2004, according to research firm Gartner. Investment in hybrid systems, which handle VoIP and conventional calls, will grow from $1.5 billion to $2 billion. By 2007, Gartner predicts, 97% of new phone systems installed in North America will be VoIP or hybrids. These statistics aren't lost on the major Internet companies. America Online, Microsoft's MSN division, and Yahoo are all entering the VoIP market, armed with services and capabilities that they've added to their popular instant-messaging software." Yahoo! Messenger is already providing voice services to millions of people. *See* http://messenger.yahoo.com/feat_voice.php;_ylt=ApTb.fq0FHxac33BwQTBaOlnMMIF.

121. *See* E911 Order, definition of "interconected VoIP."

122. FCC is planning to promptly reconsider the scope of the application of E911 requirements. E911 NPRM ¶ 58. Most observers agree that there is no principled line to be drawn between one kind of VoIP and other services that also offer voice affordances, and that it will be very difficult to limit expansions of this mandate. This means that Skype, an extraordinarily popular online voice service that has been downloaded by more than 100 million people will likely soon be subject to E911 obligations. James E. Gaskin, *What Is Skype*, O'REILLY NETWORK, Aug. 4, 2005, *available at* http://www.oreillynet.com/pub/a/network/2005/08/04/whatisSkype.html.

123. FCC CALEA order, para. 39.

like any other data stream. From an internet point of view, the E911 mandate has no principled limits and could apply to any application that is capable of connection to any public network. Although making nomadic VoIP services (much less any other data application) connect to legacy E911 hardware seems strange from an internet perspective, it fits perfectly with the mindset of people who have grown up in the telephone world. .

A darker, less public-service-oriented part of the telephony mindset is bent on squashing competitive services. Alexander Bell's own success was made possible by a strong patent and investors who were willing to fund what must have seemed like an endless flow of litigation. In the absence of an unassailable patent, today's telephony providers have had to find another approach to the enormous online voice marketplace. A cynic might find the E911 order an unprincipled and blatantly political move designed to protect the incumbents' ability to control the market for online voice services. The next section spells out the background for the cynic's view.

iii. The Capture Story

At a November 2005 telecommunications conference in Washington, D.C., Stagg Newman, a Senior Telecommunications Practice Expert with McKinsey and a former Chief Technologist at the FCC, said that he had heard that a single company wrote the E911 rule.[124] He refused to elaborate on his remarks.

Even without Mr. Newman's last word on the subject, one can see the influence of third party compliance providers in cooperation with incumbent telephony companies in the E911 rule. Third party vendors met early and often with staff and Commissioners, and filed numerous comments.[125] Intrado, the vendor that runs 80% of the selective router and E911 infrastructure in this country, met with staff to give presentations or filed comments sixteen times between April 2004 and December 2005.[126] Both Intrado and Level 3 patiently explained to staff how the E911 system functioned and how the FCC should frame its Order.[127] The FCC's June

124. Statement of Stagg Newman at pulver.com Peripheral Visionaries' IP-Based Communications Policy Summit, Nov. 10, 2005. No transcript was made of these proceedings. I was present and took notes.

125. FCC docket, WC Dkt. Nos. 04-36 and 05-196, available at www.fcc.gov.

126. Id.

127. According to Jonathan Askin of pulver.com, the FCC had considerable help in the technical parts of the Order from the firms that supply the systems used for E911 by telephone

2005 E911 Order itself cites Intrado's filings more than twenty times, and mentions that VoIP providers can use Intrado's services to connect to the dedicated hardware that is the gateway to the telephone companies' emergency services system.[128] Intrado's stock price jumped substantially during the summer of 2005.[129] With the Baby Bells and the largest non-Bell VoIP provider as its customers, and with its almost complete control over access to the required gateway to the E911 system, Intrado had every incentive to help the FCC shape the E911 rules.

Level 3, unlike Intrado, argued actively in the E911 proceeding that the Commission should be careful to take a flexible approach to compliance standards for E911 for VoIP providers, noting, for example, that "VoIP's flexibility and the growth in broadband access will lead to ever-increasing use of nomadic or mobile VoIP with added features and functionalities not available on traditional phones. . ." [130] Although the Commission declined to take this flexible route, it was no doubt comforted by the ability of Level 3 to make compliance by VoIP providers easier, as it stated in the Order that "interconnected VoIP" providers could comply with

companies. Email Askin to the author, Dec. 22, 2005. Even without this secondhand report, the ex parte filings made by Intrado and Level 3, which include many Powerpoint presentations and indications of telephonic and other contacts, tell a skeletal story of influence. Many of these filings are too summary to be helpful, however. For example, days before the E911 Order was adopted, Intrado representatives spoke to FCC staff. Here is the full report of that call in the ex parte filing made by Intrado: "On May 3, 2005, Stephen Meer, Chief Technology Officer of Intrado Inc. ("Intrado"), spoke telephonically with Julie Veach, Christi Shewman and Nicholas Alexander of the Wireline Competition Bureau to discuss 9-1-1 service provisioning for Voice Over Internet Protocol, specifically relating to New York City. Additional items discussed included ownership of telephone number blocks and 9-1-1 data management scenarios." May 5, 2005 letter Intrado to FCC. A July 2005 call, held after the E911 Order was finalized, was reported as follows: "In this meeting, Intrado relayed its commitment to working with all parties to assist in meeting the Commission's rules regarding VoIP and E911. Intrado also discussed issues related to implementation with the Commission and highlighted the cooperative efforts involved in the deployment of VoIP E911 services in New York City." Jul. 21, 2005 letter Intrado to FCC. What "issues related to implementation"? What "service provisioning"? It is clear that Intrado had influence. It is not clear what Intrado said to FCC.

128. *In the Matters Of IP-Enabled Services and E911 Requirements for IP-Enabled Service Providers*, WC Dkt. Nos. 04-36 and 05-196, *First Report and Order and Notice of Proposed Rulemaking*, rel. Jun. 3, 2005, at ¶ 38.

129. Intrado's stock was flat at 12 from 1998, when it went public, until June 2005. In June 2005 (after the E911 Order was announced, but before the Order was released), its stock price went up to 15; as of December 21, 2005, Intrado's stock price was 22.69. Gene Marcial, *The Lines Ring Off the Hook at Intrado,* BusinessWeek, Aug. 1, 2005; Hoover's detailed quote, Dec. 21, 2005 (available at http://www.hoovers.com/free/co/fin/stockquote.xhtml?COID=56660&ticker=TRDO).

130. In the Matters of IP-Enabled Services, E911 Requirements for IP-Enabled Services, WC Dkt. No. 04-36, WC Dkt. No. 05-196, Reply Comments of Level 3, Sept. 12, 2005, at 3.

the Commission's mandate in most of the households in the country by buying Level 3's wholesale E911 services.[131] Level 3 pushed the Commission to require E911 services of VoIP providers, at least for those services that competed with traditional telephone services and for which consumers had an expectation of such access.[132]

The incumbent telephone companies underscored the availability of these third party 911 solutions in their own presentations,[133] while emphasizing their own abilities to provide E911 services to their VoIP subscribers.[134] Meanwhile, both third party service providers and public safety officials noted that VoIP operators were not paying for emergency call centers via user fees – but that third party solution providers were making such contributions.[135] All of this must have satisfied the Commission that compliance with the E911 mandate made sense for VoIP providers, given that so many third parties stood ready to assist them to reduce the complexities inherent in connecting one-by-one with all of the emergency call centers in the country.

Before permitting the 2005 mergers of SBC/AT&T and MCI/Verizon to close, the FCC apparently required that AT&T, MCI, and Verizon file nomadic VoIP E911 compliance plans.[136] Each of these plans stated that the entity would no longer market VoIP products to customers in areas in

131. E911 Order at ¶38, citing Level 3, E-911: Enhanced 911 for VoIP, http://www.level3.com/userimages/dotcom/pdf/Level_3_E-911_Fact_Sheet.pdf (stating that Level 3 offers certain types of VoIP providers the ability to provide full E911 service for approximately 60% of the U.S. households with plans to support 70-80% later in 2005). Level 3 met with the Commission or filed comments more than 40 times in the E911 proceeding, and the Commission referred to Level 3 fifteen times in the E911 Order.

132. Level 3 Comments at 3, 25.

133. E.g., BellSouth ex parte presentation dated May 12, 2005, at 4 ("BellSouth will provide database services via Intrado which includes edits, posting, and return of errors for resolution by the VoIP provider."); Verizon ex parte presentation dated May 16, 2005, at 4 (showing "Intrado Gateway" to E911 system).

134. BellSouth and Verizon presentations cited in n.122, supra. SBC Aug. 15, 2005 ex parte at 18 ("Even before the Commission adopted the VoIP 911 Order, SBC and other ILECs were already offering a variety of 911 services directly to VoIP providers.")

135. Telecommunication Systems ex parte presentation, Apr. 22, 2005, at 23; Association of Public Safety Communications Officials International, Inc. ex parte letter, Nov. 30, 2005 (notes that only those service providers paying state level emergency fees should be permitted to have access to the numbers needed for nomadic VoIP users to trigger emergency responses). TCS also noted in a later presentation that public safety officers reap almost $1 per subscriber line in revenues, and are worried about that funding decreasing.

136. *See* letter Robert Quinn, AT&T, to Marlene Dortch, FCC, in WC Dkt. Nos. 04-36 and 05-196, Oct. 7, 2005; letter Richard Whitt, MCI, to Marlene Dortch, FCC, Oct. 21, 2005; letter Susanne Guyer, Verizon, to Marlene Dortch, FCC, Oct. 21, 2005.

which E911 services were not available,[137] and at least two of these plans (AT&T and Verizon) announced compliance solutions that relied entirely on Intrado-provided services. The FCC then applauded these plans and strongly urged other VoIP providers to follow their model.[138] The implicit bottom line: any non-Bell, non-Vonage independent VoIP provider would need to sign up with Intrado's services (whatever their cost), or another third-party's services, and stop marketing to customers who would not be able to receive E911 services.[139] The combination of the presence of Intrado and Level 3, with their long customer lists and control over the selective routers, together with the desire of the Baby Bells to avoid competition from upstart independent VoIP providers, provided an irresistible impetus for the resulting FCC rule.

A further capture wrinkle makes the story even plainer: In a public session held at CompTel on December 14, 2005, FCC Chairman Martin told an audience of local telephone companies (non-Bell companies attempting to compete with the Baby Bells) that the E911 Order had created enormous market opportunities for them. Why? Because, like Intrado, these local telephone companies can qualify as "telecommunications carriers." VoIP providers, by contrast, are "information services." Only "telecommunications carriers" can be certified to connect directly to the incumbents' selective routers—the hardware that accesses the special legacy emergency system that VoIP providers are required to use according to the E911 Rule. Indeed, the

137. The plans also uniformly stated that existing VoIP customers in areas not served by 911 would be "grandfathered," and that per-grandfathered-subscriber contributions would be made to local emergency services organizations – ranging up to $1.00 per grandfathered subscriber per day *See* letter Robert Quinn, AT&T, to Marlene Dortch, FCC, in WC Dkt. Nos. 04-36 and 05-196, Oct. 7, 2005; letter Richard Whitt, MCI, to Marlene Dortch, FCC, Oct. 21, 2005; letter Susanne Guyer, Verizon, to Marlene Dortch, FCC, Oct. 21, 2005.

138. *See* Enforcement Bureau Outlines Requirements of November 28, 2005 Interconnected Voice Over Internet Protocol 911 Compliance Letters, WC Docket No. 04-36, WC Docket No. 05-196, Public Notice, DA 05-2945, rel. Nov. 7, 2005, wherein the Enforcement Bureau discusses the compliance plan that AT&T is implementing to address this problem.

139. The Commission's adjuration that VoIP firms stop marketing to customers (or accepting new customers) in "all areas where they are not transmitting 911 calls to the appropriate PSAP in full compliance with the Commission's rules" (supra n. 41) is a very telephony-minded approach that raises fascinating questions. Although telephone companies know who their customers are (because they run physical, centrally-controlled networks), online VoIP providers cannot limit who sees their online advertisements. VoIP providers could perhaps comply with this FCC marketing ban by placing disclaimers on their online advertisements ("this service may not be available in all areas"), but that suggestion raises yet another question: is the FCC becoming an advertisement regulator? Isn't that the terrain of the Federal Trade Commission? In effect, the FCC is mandating that VoIP providers post ads stating, "Buy our service. It may kill you."

incumbent Bell companies *must* by law provide interconnection to these companies. Martin suggested that this was a positive development for these companies:

> 'That [selling retail access to VoIP providers to selective routers] is probably a business opportunity for many of the carriers that are out there,' Martin said . . . 'I have continued to believe that the competitive carriers are going to play an important role and many of our rules and regulations should be viewed as actually an opportunity for people.'[140]

This is a breathtaking statement. This means that the FCC was not only pushing for VoIP providers to be obligated to go through the legacy system—a solution that was bad enough in itself—but further mandating as a practical matter that they had to work with middlemen. (Recall that the FCC did not require in the E911 Order that the Baby Bells open up their selective routers to VoIP companies.)[141] And, to boot, FCC was propping up the middleman-market as an "opportunity" for its familiar regulated entities, telephone companies.

If the Commission was captured along these lines, it was not necessarily acting corruptly. The widely-reported Vonage-related deaths in 2005 may have made the FCC's telephony-minded staff feel that it was imperative to act quickly. Those who are steeped in telephony strongly believe that any communications service offered to the public must provide access to emergency officials and that technological developments must not be allowed to avoid this regulatory requirement. This point was made very clear at that dramatic May 2005 FCC meeting on the day of the adoption of the E911 mandate.[142]

140. Drew Clark, *FCC Chief Tells VoIP Firms More Regulation is an Option,* National Journal's Technology Daily, Dec. 14, 2005.

141. E911 Order, ¶ 40 (no mandate for interconnection; FCC merely says "We expect and strongly encourage all parties involved to work together to develop and deploy VoIP E911 solutions"). During this same session, Chairman Martin rejected the notion that legislation was needed to require the Bells to open connections to their selective routers to VoIP providers. Congress has been considering such legislation (S. 1063). Chairman Martin also implicitly rejected the notion, advanced by VoIP providers, that the Commission should appoint of an independent administrator of the emergency numbers that nomadic VoIP providers need to work with this hardware. Drew Clark, supra n. 137. No such administrator was needed, apparently, because Level 3 and other middlemen would provide interconnection services to the VoIP providers. Id.

142. During that meeting, one local emergency services employee said, passionately: "We should never allow an embedded base of technology subscribers and users to grow out of control

Given all the actors involved and the telephony mindset of staff, the stars were aligned in such a way that the Commission was emboldened to adopt what it itself termed an "aggressive" strategy.[143] Arguably, the Commission's E911 order was flatly impossible to implement by independent VoIP providers and deeply favored the incumbent Baby Bells. The Order also represented a missed opportunity. Development of more flexible IP-based emergency response systems, which might have been extremely helpful to consumers, was nipped in the bud.

C. *CALEA*

As with the E911 story, the CALEA controversy and the FCC's adoption of the CALEA Order in August 2005 represents a wealth of missed opportunities, permission-culture regulatory heavyhandedness, and willful misreadings of statutory requirements. If law enforcement wants access to data, they can clearly get it without insisting that it be in pre-digested form.[144] Forcing data into forms that fit the era of telephony requires forcing applications to collect recognizable data—which in turn will require those applications to be designed, in advance, to meet the desires of law enforcement.

---

before wrestling the technological and policy challenges to the ground. Any technology, any service offering, any entrepreneurial venture, that would seek to gain acceptance from the public should always have 911 and access to emergency services as its first item on the checklist before products and services are delivered to the consumer." FCC open meeting, May 19, 2005, statement of John Melcher, Executive Director, Greater Harris County (Texas) 911 Emergency Network. It is hard to imagine that all online services (including newspapers and banks) should come provisioned with E911 service, but the telephony mindset might lead in this direction. In introducing Mr. Melcher, Chairman Martin referred to the "invasion" of voice over IP services.

143. E911 Order, at ¶ 37 ("While 120 days is an aggressively short amount of time in which to comply with these requirements, the threat to public safety if we delay further is too great and demands near immediate action.") In a recent paper, J. Scott Marcus has expressed his amazement at the heavy-handedness of the E911 VoIP edict, saying: "What is striking in the case of the emergency services order . . . is the degree to which it imposes harsh, lopsided, even Draconian regulation on new market entrants. . . . Given the VoIP industry's active engagement with the emergency services community, and their significant investment in customer education on this point, it is difficult to understand the rationale." J. Scott Marcus, *Is the U.S. Dancing to a Different Drummer*, 60 Comm'ns & Strategies 39 (4th Quarter 2005) (discussing differences between U.S. and European telecommunications regulatory approaches).

144. The traditionally cooperative nature of the relationship between telcos and law enforcement is well-known, and has recently become the subject of broad public scrutiny. *See* Scott Shane, *Attention in N.S.A. Debate Turns to Telecom Industry*, New York Times, Feb. 10, 2006 ("Some [telecommunications] companies are said by current and former government officials to have provided the eavesdropping agency access to streams of telephone and Internet traffic entering and leaving the United States.").

i. *Background*

The 1994 CALEA statute "requires telecommunications common carriers to ensure that new technologies and services do not hinder law enforcement access to the communications of a subscriber who is the subject of a court order authorizing electronic surveillance"[145] by mandating that they be able to "expeditiously isolat[e] and enabl[e] the government, pursuant to a court order or other lawful authorization, to access call-identifying information that is reasonably available to the carrier. . . " and then deliver intercepted communications and call-identifying information to the government "in a format such that they may be transmitted . . . by the government to a location other than the premises of the carrier."[146]

CALEA was a heavily-negotiated statute that attempted to ensure that digital telephony services would be designed so as to be tappable by law enforcement. It authorized the Federal government to pay $500 million in industry's costs incurred before 1995 to bring telephony facilities into compliance with law enforcement's interception requirements.[147] But CALEA was written *not* to apply to "information services," defined to be services "generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications," including services "that permit[] a customer to retrieve stored information from, or file information for storage in, information storage facilities" – in other words, the internet or online applications.[148] It bears repeating: The internet and online applications were specifically excluded from CALEA's coverage.[149]

The CALEA Order released in August 2005 interprets CALEA to mean that any services provided by non-telephone companies that are in

145. CALEA Legislative History, H.R. Rep. No. 103-827(I), reprinted in 1994 U S C.C A N. 3489, 3496.

146. CALEA Sec. 103(a)(2), (3).

147. CALEA Sec. 110.

148. CALEA Sec. 102(6).

149. *See, e.g.,* House Report 103-827, *Telecommunications Carrier Assistance to the Government*, Oct. 4, 1994, at 18, 23 ("[T]he capability requirements only apply to those services or facilities that enable the subscriber to make, receive or direct calls. They 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."); *In the Matter of Communications Assistance for Law Enforcement Act*, CC Dkt. No. 97-213, Second Report and Order, rel. Aug. 31, 1999, at 7.

some way (however minor) replacements for telephone services are themselves covered by CALEA.[150] As I have explained elsewhere,[151] this interpretation is at best tenuous. Although it is true that CALEA defines covered "telecommunications carriers" to include entities (1) engaged in providing switching or transmission services (2) to the extent that the Commission finds such services to be "a replacement for a substantial portion of the local telephone exchange service," the statute also clearly *excepts* "information services" from the definition of "telecommunication carrier."[152] And broadband providers and VoIP applications (as well as any other internet application) are clearly "information services" – indeed, the FCC has said so on many occasions.[153]

The idea behind the statute was to provide law enforcement faced with digital phone systems with the tappability they had been used to with analog and mechanical phone systems.[154] Although so far there is no evidence that law enforcement is having difficulty implementing warrants for information from broadband providers or VoIP applications,[155] law enforcement asked the FCC to "clarify" its reading of CALEA to include these companies.[156] Law enforcement takes the view that because these

150. CALEA Order, ¶ 10. FCC Commissioner Copps acknowledged the strangeness of the Commission's argument on the "substantial replacement" point, saying "To me, it strains credibility to suggest that Congress intended 'a replacement for a substantial portion of the local telephone exchange' to mean the replacement of ***any*** portion of any individual subscriber's functionality." CALEA Order, Statement of Commissioner Michael J. Copps, concurring (emphasis in original).

151. Susan P. Crawford, *Shortness of Vision*, supra n.___.

152. 47 U.S.C. § 1001(8) (definition of "telecommunications carrier").

153. E.g., DSL Order, *supra* n.__. (classifying wireline broadband Internet access service (DSL) as an information service under Communications Act).

154. CALEA does not replace electronic surveillance laws; it was intended to supplement those laws. All entities are required to cooperate with law enforcement warrants and subpoenas. CALEA addresses only the question of what affordances are required of covered entities in advance of any specific warrant.

155. BellSouth cited an April 2004 audit report of the Department of Justice that stated: "[T]he FBI was unable to provide the [Auditor] with data showing the extent to which state and local law enforcement has been unable to conduct electronic surveillance as a result of these delays [in implementing CALEA solutions.]" BellSouth comments at 2-3, citing Implementation of the Communications Assistance for Law Enforcement Act by the Federal Bureau of Investigation, U.S. Department of Justice, Office of the Inspector General, Audit Division, Audit Report 04-19, at 6 (April 2004).

156. Law enforcement initially asked for a declaratory ruling rather than a rulemaking with respect to the CALEA scope issues. FCC declaratory rulings are supposed to terminate a controversy or remove uncertainty regarding the application of existing laws. 47 C.F.R. § 1.2. Law enforcement may have gone this route in order to avoid the notice-and-comment rulemaking that would be required by the Administrative Procedure Act for the promulgation of new rules or changes to existing rules. 15 U.S.C. § 553. The Commission proceeded, however, to issue a

new technologies and services are relied on by the American public, CALEA should apply to them[157]--even though the CALEA statute itself appears to specifically exclude them.

In response to law enforcement's requests, in the fall of 2005 the FCC issued its CALEA Order.[158] The CALEA Order stated generally that CALEA applies to all facilities-based broadband internet access providers (including wireless, DSL, and cable) and providers of "interconnected VoIP" services. The Order included within its scope all VoIP applications that are *capable of* connecting to the traditional telephone network, even if they do not actually connect.[159] In addition, the Commission (prompted by law enforcement) appears to be taking the position that all private broadband networks that are capable of connecting to the public internet are also covered by the FCC's interpretation of CALEA.[160] The FCC

Notice of Proposed Rulemaking concerning CALEA's scope. CALEA Order at ¶ 5 ("The Commission declined to issue a declaratory ruling, finding instead that it was necessary to compile a more complete record on the factual and legal issues surrounding the applicability of CALEA to broadband Internet access services and VoIP services, and thus issued a Notice of Proposed Rulemaking.")

157. *See* FAQ on www.askcalea.net, managed by the CALEA Implementation Unit (CIU) of the Electronic Surveillance Technology Section, a section of the Operational Technology Division, Federal Bureau of Investigation..

158. CALEA Order. As I have explained elsewhere, the FCC's issuance of the CALEA NPRM and subsequent CALEA Order was very likely a quid pro quo for DOJ's willingness to take the BrandX 9th Circuit decision to the Supreme Court on the Commission's behalf. Susan P. Crawford, *Shortness of Vision*, supra n.___. The DOJ is the FCC's lawyer for petitions for certiorari, and likely refused to take Brand X to the Supreme Court without a clear understanding with the FCC as to how "information services" would be treated under CALEA. Section 402(j) of the Communications Act and section 2350(a) of the Judicial Review Act give the Commission the right to file petitions for writ of certiorari. But, "[u]nder current practice, the Commission coordinates its petitions with the Solicitor General." Breger & Edles, 52 Admin. L. Rev. 1111, at 1251. Litigation authority matters. When the DOJ wields litigation authority, the President can ensure that "government" speaks with a single voice. *See* Neal Devins, *Political Will and the Unitary Executive: What Makes an Independent Agency Independent?*, 15 Cardozo L. Rev. 273, 274 (1993); Neal Devins & Michael Herz, *The Battle That Never Was: Congress, the White House, and Agency Litigation Authority*, 61 Law and Contemporary Problems 205 (1998) ("For DOJ and agency lawyers, [the question of litigation authority] is of monumental importance. For members of Congress and their staff, however, this question is almost always a nonstarter.")

159. CALEA Order, ¶ 39 ("To be clear, a service offering is "interconnected VoIP" if it offers the capability for users to receive calls from and terminate calls to the PSTN; the offering is covered by CALEA for all VoIP communications, even those that do not involve the PSTN.") The CALEA Order generally adopted the E911 Order's definition of "interconnected VoIP," CALEA Order at ¶ 39, and indicated that the definition of "interconnected VoIP" might itself expand over time. Id., ¶ 39 n.108.

160. CALEA does not apply to "equipment, facilities, or services that support the transport or switching of communications for private networks." 47 U.S.C. § 1002(b)(2)(B). But n.100 of the CALEA Order appears to eviscerate this private network exception, by stating that any networks that are *capable* of connecting to the internet, and any "facilities" involved in these networks, are covered by CALEA. This broadening of CALEA in n.100 of the CALEA Order, using notions

announced in the CALEA Order that it would issue a second order (on an unstated timetable) addressing the standards for CALEA compliance.[161] The generally-accepted wisdom of FCC-watchers was that the FCC would not refuse any requests law enforcement made for particular elements of compliance.

FCC Commissioner Abernathy noted the weakness of the FCC's legal claim at the time the CALEA NRPM was issued, saying:

> The NPRM we are issuing proposes a plausible interpretation of the "substantial replacement" provision in CALEA that would extend the assistance-capability requirements to broadband access services and IP telephony. But such an extension clearly would be fraught with legal risk. *The Commission thus would benefit greatly from further congressional guidance in this area.*[162]

She again expressed her concern when the Order was released, 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.[163]

There has to date been no further congressional guidance on this point. It is likely that the FCC will extend the scope of its CALEA requirements even beyond "interconnected VoIP" (defined in the E911 proceeding to mean applications that are capable of both receiving calls from and making

taken directly from the DOJ's Reply Comments in this proceeding (DOJ Reply Comments, filed Dec. 21, 2004 at 18), and has caused universities and other private network providers to sue the FCC. See text and notes infra. Arguments against n.100 are entirely separate from the "information services" attack on the CALEA Order. It is not clear what precisely is meant by "facilities that support the connection of the private network" to the internet. This notion was suggested in DOJ's reply comments, see infra text and notes at __.

161. CALEA Order, ¶ 3.

162. Action by the Commission August 4, 2004, by Notice of Proposed Rulemaking and Declaratory Ruling in ET Docket No. 04295 (FCC 04-187), Separate Statement by Commissioner Abernathy (emphasis supplied).

163. CALEA Order, Separate Statement by Commissioner Abernathy.

calls to the traditional telephone network) to other online applications with fewer direct connections to traditional phone numbers.[164]

ii. Implementation Difficulties

The Order sets a definite date for broadband facilities providers and "interconnected VoIP" providers to comply with CALEA: Eighteen months following November 15, 2005 (or in May 2007), covered entities will be subject to $10,000 fines for each day they are not in compliance .[165] The trouble is, however, that no standards have been set making clear what CALEA "compliance" means for newly-covered entities. By making compliance begin before defining what companies must to do comply, the Commission has put technology providers in an extremely difficult position; they may end up investing in compliance measures that are later found to be unnecessary, or building in elements that later need to be retrofitted to fit a mandated compliance scheme.[166]

As an initial matter, it was unclear exactly what entities were covered by the Order, given its murkiness on the subject of "private networks"[167] and CALEA's apparent complete exclusion of "information services." Also, there are many outstanding questions under the general heading of "compliance." What is "call-identifying information" for broadband providers? Although Section 102(2) of CALEA defines "call-identifying information" as "dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber by means of any equipment, facility, or service of a telecommunications carrier,"[168] that definition does not necessarily fit the online world.[169] Under current surveillance statutes, the content of

164. E911 NPRM, ¶ 58 ("Are there any other services upon which the Commission should impose E911 obligations?"); CALEA Order at ¶ 39 n.108 ("To the extent that the Commission modifies its definition of interconnected VoIP in the future, the CALEA obligations we establish today for interconnected VoIP providers will reflect such modifications.")

165. CALEA Order, ¶ 3 ("Because we acknowledge that providers need a reasonable amount of time to come into compliance with all relevant CALEA requirements, we establish a deadline of 18 months from the effective date of this Order, by which time newly covered entities and providers of newly covered services must be in full compliance.")

166. *See infra* n.__ [former n.169).

167. *See* n.__, *supra.*

168. 47 U.S.C. § 1001(2).

169. In the CALEA Order, the Commission said that this and other questions would be answered in a forthcoming Order, including "the ability of broadband Internet access providers and VoIP providers to provide all of the capabilities that are required by section 103 of CALEA" and "what those capability requirements mean in a broadband environment." CALEA Order, ¶ 46. Section 103 broadly requires covered entities to ensure that their equipment, facilities, and

communications may not be made available to government entities absent appropriate warrants. But because all online packets contain both "header" information (about routing) and "payload" or content information, it is not clear how CALEA's mandate can be complied with by online services. CALEA's requirements that the privacy of subscribers be protected and that call-identifying information may not include "any information that may disclose the physical location of the subscriber"[170] further complicate this question for online applications.[171]

What new designs will be required of VoIP applications? What information is "reasonably available" to these entities?[172] The goal of the statute is to standardize the forms of data delivered to law enforcement, but covered entities were not told by the Commission what forms of data would be acceptable. The FCC expressly deferred to later Orders any statement as to what compliance means or what exemptions from coverage might exist.[173]

The implementation of CALEA in the telephone world has been (and continues to be) extremely difficult. An initial industry-created standard for telephony compliance (the J-standard) was rejected by law enforcement, who then proposed an elaborate "punchlist" of desired compliance elements.[174] This punchlist led to extensive litigation and further FCC action over more than a decade.[175] Now, in the online context, law enforcement has declared that compliance standards will be set by

services enable interception, isolate call-identifying information "that is reasonably available to the carrier," allow this information to be delivered to law enforcement in an approved format, and protect subscribers' privacy and the confidentiality of the interception.

170. Sec. 103(a)(2)(B), (a)(4). Specifically, Sec. 103(a)(4) states that common carriers should not disclose "call-identifying information" that is "not authorized to be intercepted." The Commission has said that "privacy concerns could be implicated if carriers were to give to [law enforcement agencies] packets containing both call-identifying and call content information when only the former was authorized." Communications Assistance for Law Enforcement Act, Third Report and Order, 14 F.C.C.R. 16,794, para. 48 (1999).

171. *See* Shortness of Vision, noting that IP addresses may in fact reveal the physical location of users.

172. CALEA does not define or interpret the term "reasonably available."

173. CALEA Order, ¶ 3 ("In the coming months, we will release another order that will address separate questions regarding the assistance capabilities required of the providers covered by today's Order pursuant to section 103 of CALEA. This subsequent order will include other important issues under CALEA, such as compliance extensions and exemptions, cost recovery, identification of future services and entities subject to CALEA, and enforcement.")

174. For the history of this battle, *see* FCC Third Report and Order, *In the Matter of Communications Assistance for Law Enforcement Act*, CC Dkt. No. 97-213, rel. Aug. 31, 1999.

175. *Id*.

industry, with law enforcement and the FCC to decide later whether those standards were deficient or not.[176]

This method of proceeding (decide generally who is covered by CALEA, using dubious legal reasoning, without deciding what standards of compliance apply to those entities) creates enormous risks for entities newly covered by CALEA. If they are found in the future to have built products considered "deficient" by law enforcement, they will run the risk of having their services taken off the market and incurring enormous fines. Indeed, law enforcement emphasized to the FCC that service providers should build their systems in the first place to be CALEA-compliant, because it would be expensive to have to retrofit them later.[177] All prudent businesses will want to run their services by law enforcement, suggested 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 certainly consider a service provider's failure to request such guidance in any enforcement action.[178]

This is a threat: come negotiate with us first, or you will run the risk of being subject to penalties later. It flies in the face of the legislative history of CALEA, for Congress said when the statute was adopted that "if a service of [sic] technology cannot reasonably be brought into compliance with the interception requirements, then the service or technology can be deployed," and rejected "original versions of the legislation, which would have barred introduction of services or features that could not be tapped."[179]

But service providers reading the CALEA Order had to take law enforcement's pre-approval approach seriously, because it was very apparent that law enforcement was feeling powerful. This was extremely awkward for technology providers, because they were unsure what the

176. Reply Comments of the Dept. of Justice, *In the Matter of Communications Assistance for Law Enforcement Act and Broadband Access and Services*, ET Dkt. No. 04-295 (filed Nov. 8, 2004), at 58 (arguing that DOJ prefers to use the deficiency petition process to resolve standards disputes).

177. Id. at 44-45.

178. Id. at 36, 38.

179. House Report at 3499.

standards were to which they were going to need to build, and, in some cases, whether they were covered by the statute's mandates in the first place. The CALEA Order arguably created a cloud over innovation and product development, particularly for smaller technology providers who might be unable to bear the costs of potentially unlimited compliance requests by law enforcement.[180]

For example, Pulver.com makes a free service called Free World Dialup available to the public. Free World Dialup uses peer-to-peer connections between people communicating, but is capable of connecting to the traditional telephone network. Because the CALEA Order appears to require any application that can interconnect with the telephone network to be CALEA-compliant, Pulver.com will have to consider withdrawing the Free World Dialup service if it is determined to be subject to the Order. Because it is a free service, no compliance costs are bearable. But Pulver is unsure whether CALEA applies to Free World Dialup, and has therefore decided to cease to provide FWD in the U.S..[181] Similarly, Skype is a peer-to-peer application that has been downloaded by more than 150 million people.[182] Subscribers can purchase from Skype the ability to connect to traditional telephone numbers, and to receive calls from traditional telephone subscribers. It is unclear whether Skype is covered by CALEA.[183]

Although the first CALEA order issued by the FCC covers only scope—the question of which entities are considered by the FCC to be obligated to comply with CALEA—law enforcement will in the coming months dictate to the FCC its strong view of the mandatory requirements to

180. For example, a small business making mesh network access available to rural areas (by providing equipment that allows each computer to seek out other nodes that may or may not be connected to the internet) might be forced under the CALEA Order to comply with unpredictable "punchlist" demands by law enforcement, and would likely respond by going out of business. And CALEA compliance would likely be nearly impossible for open source projects that always publish their code publicly. *See* CDT Comments In Support of the Petition for Reconsideration and Clarification of the CALEA Applicability Order filed by USTA. [date filed]

181. Greg Piper, *Groups Ask Appeals Court to Overturn FCC CALEA Order*, Comm. Daily, Oct. 26, 2005. As noted above, pulver.com has "chosen not to offer a PSTN-connected VoIP service in the US because of the FCC's backward-looking, anti-innovative rules on E-911 and CALEA." Email Jonathan Askin of pulver.com to the author, Dec. 20, 2005.

182. In late 2005, Skype was purchased by eBay for $2.6 billion. Richard Waters and Paul Taylor, *Ebay, Skype Deal Challenges Rivals*, FT.com, Sept. 12, 2005.

183. Ryan Singel, *Furor Grows Over Internet Bugging*, Wired News, Oct. 20, 2005 (noting that CALEA Order "appears to pull in" Skype; Skype did not return a call seeking comment).

be applied to the internet and VoIP applications.[184] They will seek to declare what information they want and the limited number of standardized interfaces in which they are willing to receive it. And, of course, VeriSign stands ready to provide those data fields to law enforcement. Indeed, law enforcement has cited VeriSign's service pitches in arguing that CALEA compliance will not be expensive and that therefore the costs for such compliance can easily be borne by the businesses they believe are covered by the CALEA statute.[185]

Soon after the CALEA Order was published, five sets of parties sought to have it stayed or reversed by the D.C. Circuit.[186] For example, the American Council on Education (ACE), a trade association for institutions of higher education in the U.S., filed a lawsuit on Oct. 24, 2005, alleging that the Order would cause a $7 billion upgrading expense to colleges and universities who provide broadband access to others.[187] ACE argued that the "incredible cost of compliance" made the Order an inefficient approach to assisting law enforcement.[188] ACE also noted that CALEA cannot be read to apply to providers of facilities that connect private networks to public networks, because Congress made clear in the statute that CALEA requirements do not apply to "equipment, facilities, or services that support the transport or switching of communications for

184. The FCC announced in the CALEA Order that it would issue a second order (on an unstated timetable) addressing the standards for CALEA compliance. CALEA Order, ¶ 3. The generally-accepted wisdom of FCC-watchers was that the FCC would not refuse any requests law enforcement made for particular elements of compliance.

185. Law Enforcement Joint Reply Comments, RM-10865, filed Apr. 27, 2004, at 47 ("With regard to broadband CALEA compliance costs, at least one solution vendor (Verisign) stated in its comments that broadband solutions are available at reasonable prices. . as Verisign's ex parte presentation dated April 15, 2004 shows, the CALEA capital costs for VOIP and IP-enabled services appear to be minimal. The CALEA capital costs range from $100,000-405,000 per year ($0-5,000 for the access device; $100,000-400,000 for the mediation device).")

186. All of these cases were filed in the D.C. Circuit with the FCC and the United States as respondents: 05-1404, American Council on Education; 05-1408, American Library Ass'n, Association of Research Libraries, Center for Democracy & Technology, COMPTEL, Electronic Frontier Foundation, Electronic Privacy Information Center, Pulver.com, Sun Microsystems; 05-1438, American Civil Liberties Union; 05-1451, Pacific Northwest GigaPOP, Corporation for Education Network Initiatives in California, Internet2, and National LamdaRail. The cases were consolidated for expedited briefing and argument in mid-December 2005, and are scheduled to be heard in the spring of 2006.

187. Press release, *ACE Files Suit Against FCC Over New Wiretapping Regulations*, Oct. 24, 2005, available at http://www.acenet.edu/AM/Template.cfm?Section=Legal_Issues_and_Policy_Briefs2&CONTENTID=12507&TEMPLATE=/CM/ContentDisplay.cfm; Declan McCullough, *FBI Net-wiretapping Rules Face Challenges*, ZDNetNews, Oct. 24, 2005.

188. Id.

private networks." [189] The Center for Democracy and Technology, together with a large group of other civil society groups and companies, sought relief from the Order on the grounds that it exceeded the Commission's statutory authority and was arbitrary and capricious in establishing a hard deadline for compliance without saying what compliance entailed.[190] The CDT lawsuit also emphasizes the substantial risks to innovation[191] posed by having to seek approval from law enforcement before launching any potentially CALEA-covered application or network facility.[192]

iii. The Capture Story

CALEA is similar to E911 in that in both proceedings some of the incumbent Baby Bells are pushing for CALEA compliance that will burden their competitors, the VoIP providers.[193] And the key compliance vendor, VeriSign, did its best to persuade the Commission that its service bureau model would minimize any impacts on innovation that application providers might otherwise experience.[194] In the end, the Commission's

189. ACE Statement of Issues to be Raised, filed in ACE v. FCC, et al., Case No. 05-1404 (D.C. Cir.).

190. American Library Ass'n, Association of Research Libraries, Center for Democracy & Technology, COMPTEL, Electronic Frontier Foundation, Electronic Privacy Information Center, Pulver.com, Sun Microsystems v. FCC et al., Case No. 05-1408 (D.C. Cir.).

191. In addition to the risks to innovation, Susan Landau of Sun Microsystems argues in a recent paper that applying CALEA to VoIP poses substantial national security risks. Susan Landau, *National Security On the Line*, Dec. 30, 2005 (unpublished manuscript, on file with author) ("in the current communications environment, with an unsecured Internet upon which critical infrastructure depends heavily, building surveillance technology directly into Internet protocols has very negative national-security implications.")

192. CDT and its co-petitioners filed their opening brief on Jan. 26, 2006. Oral argument has not yet been scheduled.

193. Verizon filed comments strongly supporting the Commission's reading of CALEA to include VoIP providers, Verizon Comments at 5; Verizon Reply Comments at 4; and supporting the Commission's determination that law enforcement needs mandated extension of CALEA to all broadband providers, Verizon Comments at 10 (arguing that CALEA should be applied to all broadband access providers because to do otherwise would "enable individuals to avoid electronic surveillance simply by virtue of what broadband access service they choose"). SBC also pushed for CALEA requirements to be broadly applied to ensure a level playing field, SBC Comments at 7 (stating that "the Commission must ensure that the application of CALEA is competitively neutral . . . [a]ll service providers, regardless of the platform they use to deliver the services (i.e., cable, DSL, wireless, satellite, powerline), should be subject to the same CALEA obligations").

194. VeriSign made clear to the Commission that it already had a compliance service in the marketplace. *See* letter VeriSign to Marlene Dortch, FCC RM-10865, Jul. 16, 2004 ("VeriSign is a globally recognized leader in providing an array of large-scale, ultra-high availability infrastructure support capabilities for traditional voice telecommunications, Internet, security, and financial transaction services to providers and consumers through its various divisions in the U.S.

CALEA Order did recognize that "[i]ndustry solutions" for compliance with CALEA "appear to be readily available."[195]

VeriSign did more than simply hawk its services, however (although it did that with astonishing bravado); it also worked hard to persuade the Commission that the U.S. was lagging behind other countries in its support for law enforcement lawful access to communications.[196] For example, in a presentation by VeriSign in July 2004, the company stated several times that the Commission's action on CALEA for broadband and VoIP was needed in order to align with "worldwide requirements" and "worldwide related activities and actions."[197] VeriSign told the Commission that "Next Generation Network" standard-setting activities around the world required that CALEA mandates be put in place.[198]

Even after the Commission issued its CALEA order in September 2005, VeriSign continued to agitate for better treatment. It suggested (while reminding the Commission of its existing compliance service bureau offering) that all providers of VoIP services (not just those interconnecting with the traditional telephone network) be covered by the mandate.[199] VeriSign urged the Commission to hurry up with the implementation of its order, saying that VeriSign had been *relying* on the Commission's

and worldwide. As part of these commercial infrastructure support services, it provides NetDiscovery Services™ to wireless, wireline, cable, satellite, and IP-enabled service providers as a cost-effective means of meeting CALEA obligations (and the equivalent in other countries) through a service bureau.") Although a list of VeriSign's customers for NetDiscovery is not public, Vonage and Cox Communications have both adopted this service. Press release, VeriSign Net Discovery Services Selected by Vonage, San Jose, Calif. (Mar. 8, 2005); Press release, VeriSign NetDiscovery Services Implemented by Cox Communications, Mountain View, Calif. (Apr. 5, 2004). Vonage is far larger than the other VoIP players.

195. CALEA Order at 22 & n.127.

196. E.g., VeriSign reply comments, ET Dkt. No. 04-295, filed Apr. 27, 2004 ("the capabilities sought by law enforcement have been available for more than a decade, and deployed on an ad-hoc basis in the U.S. over that period. In some G8 countries, this has occurred on a national scale.")

197. Letter VeriSign to Marlene Dortch, RM-10865, Jul. 16, 2004 (attaching presentation).

198. *Id*. "Next Generation Network" is an umbrella term for the kind of network that incumbent telephone companies and cable companies would like to substitute for the public internet. It is characterized by services that, much like those provided by mobile phone companies, can be easily tracked and charged for; it is a "walled garden" that is controlled by the service provider. According to Wikipedia, "The general idea behind NGN is that all information is transmitted via packets, like the Internet; packets are labeled according to their type (data, voice, etc) and handled differently for QoS [quality of service] and security purposes by traffic management equipment." http://en.wikipedia.org/wiki/Next_Generation_Networking

199. *In the Matter of Communications Assistance for Law Enforcement Act and Broadband Access Services,* ET Dkt No. 04-295, RM-10865, Comments of VeriSign, Inc., Nov. 14, 2005, at 2.

imposition of CALEA on a broad range of applications and services.[200] It also stated that any potential incurred costs to entities covered by the CALEA mandate "can be readily outsourced with a CALEA service bureau as part of a compliance agreement" – VeriSign's service – and that these costs would quickly end if the scope of the Commission's CALEA mandate was found to be improper by a court.[201]

But the overall capture profile for CALEA is different from that for E911. Although compliance companies—most notably VeriSign—would like to ensure that their services are called for by the Order, and the FCC takes some comfort in requiring CALEA compliance of broadband providers and "interconnected VoIP" companies because of the existence of such third-party services,[202] the Commission has not yet stated what compliance with CALEA will entail. Third party providers of outsourced services are thus not as firmly in the driver's seat in the CALEA context as they are in the E911 realm: In CALEA there is no legacy infrastructure (or even a set of standards) over which a third party already has control. Third parties like VeriSign, accordingly, could promise as a "trusted third party" to install Carnivore-like black boxes to inhale all data from broadband providers and applications, and then parse it on behalf of law enforcement,[203] but whether that would be enough for law enforcement was not decided by the FCC in this initial Order. Indeed, law enforcement comments in the CALEA proceeding made clear that they wanted to

200. *In the Matter of Communications Assistance for Law Enforcement Act and Broadband Access Services,* ET Dkt No. 04-295, RM-10865, VeriSign, Inc. Opposition, Request for Stay Pending Issuance of Subsequent Orders and for Stay Pending Judicial Review, Dec. 2, 2005, at 10 ("Both VeriSign and its customers have relied in good faith on the Commission's timely imposition of necessary digital forensic capabilities under CALEA. VeriSign has made significant investments to provide the required support capabilities to its customers. . . . Petitioners' assertion [in seeking a stay of the CALEA Order] that no party will be harmed ignores the adverse effects on the many parties who developed these capabilities to meet the Commission's implementation deadline.")

201. Id. at 10.

202. CALEA Order ¶ 43 & nn. 126-127 (noting VeriSign's claim of the "ready availability [to providers of VoIP and broadband Internet access services] of high-performance, reasonably priced adjunct devices capable of supporting law enforcement needs," and citing Vonage's adoption of VeriSign's NetDiscovery services.

203. *See* Comments of VeriSign, Apr. 12, 2004, at 8 (noting use in service bureau model of "isolated adjunct devices that passively duplicate transmission streams and actively filter target communications"). VeriSign even promised to adjust to law enforcement demands without necessarily needing to consult with the covered entity. Comments of VeriSign, at 21 ("If standards do not exist, or are deemed deficient by law enforcement, or are evolving because of changed or additional law enforcement requirements, the service bureau effects necessary interim solutions to the satisfaction of law enforcement and their collection and analysis equipment vendors.")

maintain direct contact with entities covered by the statute in order to ensure compliance with all of their demands.[204]

The real story of this rulemaking is that the Commission was driven by law enforcement doggedly to rely on an unsupportable reading of CALEA. Even the Bells recognized this. As BellSouth commented:

> [N]ational security concerns should not and cannot be used as a veil for the Commission to embark upon an administrative re-write of CALEA when that statute does not grant such authority. . . . [M]any of the rules and requirements imposed in the [NPRM] are plainly inconsistent with both the language and the legislative history of the statute.. . . To the extent the needs of law enforcement have changed and communications technology has evolved since CALEA was enacted, law enforcement and the industry should work with Congress to amend the current law.[205]

The Brand X deal[206] and the heavy hand of law enforcement in the post-9/11 world pressured the FCC into doing the best it could to give law enforcement the design authority it sought, while shielding DOJ from the vicissitudes of the legislative process. In effect, the Commission (*encouraged* by law enforcement) reached the conclusion that it would apply CALEA to broadband and VoIP and then backed into the legal reasoning it needed in order to do this without Congressional authorization. But, as noted by Congress at the time CALEA was enacted, CALEA was "not intended to guarantee 'one-stop shopping' for law enforcement,"[207] and it is very likely that the lawsuits already filed will slow the broadening of CALEA that law enforcement seeks.

Again, as in the E911 setting, the Commission's actions in construing CALEA in the manner that it did were not necessarily corrupt. It is very likely that the Commission was told, as Americans are told these days in many contexts, that the FCC's failure to extend CALEA would result in a

204. *E.g.*, DOJ Reply Comments, Dec. 21, 2004, at 28-29 (entities obligated to comply with CALEA must remain fully involved in designing CALEA solutions; Commission should be reluctant to shift CALEA responsibilities to trusted third parties).

205. BellSouth Comments, Nov. 8, 2004, at 2.

206. *Supra* n.__.

207. House Report at 3502.

definitive terrorist attack on the United States. The absence of a colorable legal justification to issue the CALEA Order did not stop the FCC from acting. It undoubtedly believed it was helping those who protect United States citizens.[208]

III. NEW FORMS OF CAPTURE

The delegation by Congress of broad power over communications to an independent, unaccountable "expert" agency is leading in this age of convergence to a situation in which the capture of rulemakings about "new technology" by "old technology" companies and interests is very likely. Out of the glare of public scrutiny that would likely accompany any attempt to legislate in this area, incumbents, law enforcement, and vendors of compliance services are finding it relatively easy to extract from the Commission rules that favor them and keep the world of telephony policy in place. They would find it relatively difficult to extract these same rules from Congress, because more interest groups would be involved and more eyes would be watching. Because "innovation" does not have a lobbyist, and because the providers of online services are not as well-organized, well-funded, or well-connected as the capturers are, opposition to the Commission's initiatives is easily ignored. The mainstream press is not paying attention to the enormous power grab that is proceeding at the Commission. And there is no way to remove from office the Chairman and Commissioners who have brought these most recent rules to pass. The only way to address the FCC's actions is to sue, and both of these rules have prompted lawsuits. The aim of this Part is to summarize the pre-issuance capture story these case studies reveal, in hopes that Congress will be more careful in the future. The Part proceeds in three subsections: explanation of the delegation history for the two rulemakings, an exploration of the "expertise" of the FCC in these two areas, and the capture narrative.

208. A possible parallel looms here: the (very persuasive and powerful) content community caused FCC in the broadcast flag context to take the position that it had jurisdiction to mandate that all devices capable of receiving a digital television signal have secure digital outputs that prevented onward transmission of a marked file over the internet. In the flag context, as in the CALEA context, not having legal authority did not stop the FCC from acting.. Susan P. Crawford, *The Biology of the Broadcast Flag,* 25 HASTINGS COMM/ENT 599 (2003*)*.

A. Delegation

These two rulemakings do not have the same delegation background. In the CALEA context, it is extremely unlikely that Congress intended for broadband access and VoIP services to be covered by CALEA.[209] Thus, it is likely that the D.C. Circuit will find that no delegation has occurred, and law enforcement will need to return to the Hill in order to obtain the authority it seeks.

In the E911 world, by contrast, recent caselaw interprets the Commission's "ancillary authority" under the Telecommunications Act to give the FCC almost unlimited power over anything having to do with a wire or a radio signal in the U.S.—and thus, impliedly, over any application used online. Given the importance of the internet to the economic future of this country, Congress should act to discipline the Commission's authority; at the very least, Congress should be explicit that it is giving power over the internet to the FCC.

The Commission divides all possible radio and wire communications into two broad categories: (1) telecommunications services, regulated under Title II of the Communications Act, and required to charge tariffed fees, pay into the universal service fund, and not discriminate against others who want to connect to them; and (2) information services. The FCC has taken the position in the past that all IP-enabled services of whatever description (save for the Internet Protocol itself, or "internet governance") fit into the information services category,[210] and therefore are regulated under its general powers (including its "ancillary" powers) under Title I. Commentators have even referred to "Title I" and "Title II" services.[211]

209. *See* text and notes at ___, supra.

210. *Id.*

211. JONATHAN E. NUECHTERLEIN AND PHILIP J. WEISER, DIGITAL CROSSROADS: AMERICAN TELECOMMUNICATIONS POLICY IN THE INTERNET AGE 213 (2005). In the E911 context, the FCC finessed the classification question, saying that it had not decided whether interconnected VoIP services were telecommunications services or information services, but that it analyzed E911 primarily under its Title I ancillary jurisdiction "to encompass both types of service." E911 Order, *supra* note ___, at ¶ 22. It is astonishing for the Commission to avoid deciding (or declaring) where its authority comes from in taking a particular regulatory position. It had every political reason to approach the VoIP E911 question in this way, however; the public outcry that would have resulted if the FCC had attempted to create tariffing structures and interconnection requirements and special charges for VoIP services made the choice of Title II classification inappropriate, but the FCC's ancillary Title I jurisdiction over "interconnected VoIP" services is unclear (as I discuss below). And so the Commission spread its bets by choosing both classifications. The FCC may have wished to avoid any conflict with a 1998 FCC report (the "Stevens Report,") that reviewed VoIP services in connection with universal service

Title I contains a "necessary and proper" rulemaking provision, Section 154(i), that says that the 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."[212] This Section allows the Commission to implement regulations that are necessary to carry out its explicit responsibilities under the Communications Act, and courts have found that the FCC can exercise "ancillary authority" to adopt legislative rules using Section 154(i) when two conditions are met: (1) it otherwise has subject matter jurisdiction over the service to be regulated and (2) its regulations are reasonably ancillary to the Commission's effective performance of its statutorily mandated responsibilities.[213]

From the Commission's perspective, the only question it has to answer for the first part of this test is whether "interconnected VoIP" services specifically, or IP-enabled services generally, use wires or radios. Because they do, the FCC asserts that "these services come within the scope of the Commission's subject matter jurisdiction granted in section [152(a)] of the Act."[214] Following the Commission's logic, and read for all it is worth, Section 152(a) gives the Commission subject matter authority over all communications by wire and radio anywhere in the world.[215]

obligations. The Commission tentatively concluded in the Stevens Report that some "phone-to-phone" VOIP services "lack[] the characteristics that would render them "information services" within the meaning of the statute, and instead bear the characteristics of "telecommunications services." See *In the Matter of Federal-State Joint Board on Universal Service*, CC Dkt. No. 96-45 (Report to Congress), FCC 98-67, Apr. 10, 1998 ("Stevens Report").

212. 47 U.S.C. 154(i).

213. United States v. Southwestern Cable Co., 392 U.S. 157, 177-78 (1968) (upholding cable television regulations before FCC had express congressional grant of regulatory authority over cable). The D.C. Circuit has recently been quite skeptical of the Commission's Title I authority. When the FCC used its Title I jurisdiction to justify video description for television programs, the D.C. Circuit struck down those rules because they were outside the Commission's authority. Motion Picture Ass'n of America, Inc. v. FCC, 309 F.3d 796 (D.C. Cir. 2002). And in American Library Ass'n v. FCC, 406 F.3d 689 (D.C. Cir. 2005), the D.C. Circuit ruled that the Commission lacked authority to impose broadcast content redistribution rules on equipment manufacturers (the "broadcast flag" rules) using its Title I ancillary jurisdiction because the equipment was not subject to the Commission's subject matter jurisdiction. The FCC argued for very broad ancillary authority in the broadcast flag case, announcing 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 with respect to anything "associated with the overall circuit of messages sent and received" via wire or radio. Respondent's Brief, at 23, 25; E911 Order, *supra* note ___, at ¶ 32.

214. E911 Order, *supra* note ___, at ¶ 28.

215. Section 152(a) is about the scope of the coverage of the Act -- it intentionally excludes

As for the second step in the ancillary jurisdiction test, the Commission acknowledges in a footnote that the Telecommunications Act states that "[i]t is the policy of the United States - 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,"[216] but asserts that it does not believe that this "policy statement precludes [it] from adopting E911 rules for interconnected VoIP providers here."[217] The Commission rehearses its "safety of life and property" arguments, notes that it has in the past imposed E911 rules on providers of new telephone technologies, argues that Congress has "ratified" its exercises of authority in this area in the 1999 Wireless Act, and asserts that the Order is reasonably ancillary to the Commission's effective performance of its statutorily mandated responsibilities.

And the Commission hints in the NPRM accompanying the E911 Order that it seeks to do even more. As noted, the FCC appears to be considering whether to require any VoIP-capable device to be able by June 2006 to automatically determine its location to be provided in a E911 call.[218] The FCC is wondering whether its focus on "interconnected VoIP" services is too narrow.[219] And the Commission is considering adopting consumer privacy protections applicable to E911 service, implying that the FCC will create through regulation broad online privacy rules that to date Congress has resisted legislating.[220] It is very likely that future IP-enabled services "social policies" will be based on the same jurisdictional

people in the Canal Zone, for example -- and says nothing about rulemaking authority. Section 152(a) states that "The provisions of this chapter 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, and to the licensing and regulating of all radio stations as hereinafter provided; but it shall not apply to persons engaged in wire or radio communication or transmission in the Canal Zone, or to wire or radio communication or transmission wholly within the Canal Zone. The provisions of this chapter shall apply with respect to cable service, to all persons engaged within the United States in providing such service, and to the facilities of cable operators which relate to such service, as provided in subchapter V-A."

216. 17 U.S.C. § 230(b)(2).

217. E911 Order, *supra* note ___, at § 29 n.95.

218. *Id.*, § 57. Arguably, Congress in Section 230 of the Telecommunications Act said clearly that special federal regulation of "internet services" was inappropriate. It appears that the Commission has convinced itself that the word "regulation" in Section 230 refers only to Title II common carrier-type regulations having to do with tariffs and interconnection, and not to "social policies."

219. *Id.*, § 58.

220. *Id.*, § 62.

arguments.

The chief problem with the Commission's claims is that the jurisdictional arguments made in the E911 Order have very few principled limits. Anything that has something to do with a wire or a radio may be asserted to be within the FCC's jurisdiction, and the FCC may expand the scope of its policies at any time. Although the Telecommunications Act does not impose any explicit regulatory burdens on "information services," the FCC views itself to have complete discretion under its "ancillary jurisdiction" to decide what requirements it should mandate with respect to these services.[221]

The FCC's policy, until relatively recently, was that online services should be unregulated.[222] As it turns out, however, all services that use the Internet Protocol are "unregulated" only if you have a telephony background–they are "unregulated" in the sense that they are not classified as Title II common carrier services (subjected to tariffing and interconnection obligations), but they are regulated in reality. The E911 Order is the clearest demonstration to date that the FCC's telephony mindset drives it to believe that it has absolute discretion under Title I to impose fundamentally unchanged telephony-based mandates on certain categories of IP-enabled services.[223]

221. The FCC's views about its Title I jurisdiction have become more aggressive in recent years. In 2001, in its approval of the AOL-Time Warner merger, the Commission imposed conditions on AOL's instant messaging application (conditions that were later lifted), but based its authority on its power over approving spectrum license transfers from Time Warner's cable companies, broadcast companies, and telephony interests to the merged entity as well as on its Title I jurisdiction. *See* Applications for Consent to the Transfer of Control of Licenses and Section 214 Authorizations by Time Warner Inc. and America Online, Inc., Transferors, to AOL Time Warner Inc., Transferee, FCC 01-12, CS Docket No. 00-30, rel. January 22, 2001. This assertion of Title I jurisdiction was not tested on appeal. Today, in 2005, it is very likely that the Commission would base its authority to regulate instant messaging solely on its ancillary jurisdiction under Title I.

222. *See* Jason Oxman, *The FCC and the Unregulation of the Internet*, FCC Office of Plans and Policy Working Paper No. 31 (July 1999), available at http://www.fcc.gov/Bureaus/OPP/working_papers/oppwp31.pdf, at 22 ("As more services are offered that use the Internet Protocol in a packet-switched environment, it becomes increasingly difficult to determine where the telecommunications service ends and the information service begins. Despite this difficulty, however, it remains important for the FCC to maintain the unregulated status of data services offered over telecommunications facilities.")

223. Philip Weiser has recommended that the FCC regulate all internet services under Title I using antitrust principles. Philip J. Weiser, *Toward a Next Generation Regulatory Strategy*, 35 LOY. U. CHI. L.J. 41, 66 (2003) ("outlin[ing] how the FCC can rely on its Title I authority to employ a reactive, antitrust-like model of regulation for the emerging broadband market"). By contrast, James Speta takes the view that Title I does not stretch as far as the Commission would

The Commission's belief in its "unregulation" agenda for IP-enabled services received a substantial shot in the arm as a result of the Supreme Court's recent *Brand X* opinion.[224] Justice Thomas, writing for the Court, ruled that judicial deference to the Commission's determination that cable modem internet access service is an "information service" was appropriate. This holding was legally sound, but in dicta the Court said 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,"[225] 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).[226]

This dicta in the *BrandX* 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 adopted (like E911) look just like rules applied to common carriers. In other words, classification of services as "telecommunications," on the one hand, or "information services," on the other, has become a matter of form over substance. Even if something is called an "information service," the Commission can mandate requirements of it that used to be required only of "communications services." The opinion also signals that the internet is too difficult and complicated for any branch of government other than the FCC to deal with.[227]

Justice Scalia's stinging dissent makes the judicial grant of power to the Commission clear:

> [W]hat the Commission hath given [by classifying cable modem service as an information service], the Commission may well take away—unless it doesn't. This is a

like it to, and that the FCC's regulatory authority should be limited. James B. Speta, *FCC Authority To Regulate the Internet: Creating It and Limiting It*, 35 LOY. U. CHI. L.J. 15 (2003). The Commission appears to be listening to neither Weiser nor Speta, because it is forging ahead with non-antitrust regulation under a broad reading of Title I. It will take a substantial change in public concern over the fate of internet services and a clearly different congressional direction for the Commission to change its approach.

224. National Cable & Telecommunications Ass'n v. Brand X Internet Services et al., 545 U.S. __ , 125 S.Ct. 2688 (2005).

225. *Id*., slip op. at 3-4.

226. *Id*., slip op. at 20.

227. *Id*., slip op. at 20.

> wonderful illustration of how an experienced agency can (with some assistance from credulous courts) turn statutory constraints into bureaucratic discretions.[228]

The E911 order marks only the beginning of the Commission's regulation of the internet under its unprincipled (and potentially unlimited) reading of its ancillary jurisdiction. In this crucial area, silence (or even ambiguous statements) by Congress should not afford the Commission such enormous powers.[229] Congress should act to cabin and explicate the scope of the Commission's authority to regulate the internet. The difficult and important question of how to govern the internet should be answered explicitly rather than through formalistic recharacterization of internet services by an independent agency.[230]

B. Expertise

To the extent Congressional delegation to the FCC of powers over IP-enabled services (if such delegation occurred) was legitimate because the FCC is expert and above the political fray,[231] both the E911 and CALEA

228. *Id*., Scalia, dissenting, at 10.

229. For important questions, or questions with substantial economic impact, the Supreme Court has ruled that an agency's interpretation of an ambiguous statute should not be deferred to. FDA v. Brown & Williamson Tobacco Corp., 529 U.S. 120, 159 (2000) ("Deference under Chevron to an agency's construction of a statute that it administers is premised on the theory that a statute's ambiguity constitutes an implicit delegation from Congress to the agency to fill in the statutory gaps. In extraordinary cases, however, there may be reason to hesitate before concluding that Congress has intended such an implicit delegation.") (citations omitted). Regulation of the internet is the kind of "extraordinary case" to which the Court was referring. As in Brown & Williamson, this broad swath of regulatory power (i) addresses an important domain — regulation of a great "basic industry" — for which authority could not have been delegated accidentally; and (ii) concerns a question about which Congress has already enacted several statutes. Congress should refuse to grant such broad jurisdiction to a single, easily captured agency.

230. *See* John T. Nakahata, *Broadband Regulation at the Demise of the 1934 Act: The Challenge of Muddling Through*, 12 COMMLAW CONSPECTUS 169 (2004) (questioning the Commission's authority to create new regulatory structures for "Title I" services)("The Commission is not the Congress—it cannot enact new laws outside of the Act's delegations of rulemaking authority.")

231. Independent Agencies were supposed to be "[A] body of experts who shall gain experience by length of service—a body which shall be independent of executive authority, except in its selection, and free to exercise its judgment. . . " Marshall J. Brefer & Gary J. Edles, *Established by Practice: The Theory and Operation of Independent Federal Agencies*, 52 Admin. L. Rev. 1111, 1113 (2000) (citing Humphrey's Ex'r v. United States, 295 U.S. 602, 625-26 (1935) (internal quotation marks and citation omitted). "[T]he independent commission as an organizational form did not emerge full-blown with the passage of the Interstate Commerce Act. Rather, it evolved over the course of several decades, coming to maturity late in the Progressive

rulemakings substantially undermine this theory.

It is not just that the Commission needed the technical assistance of Intrado and VeriSign to write these rules—agency resource limitations often dictate that the help of outside parties is called for. It is not just that the Commission was forced into the CALEA rulemaking as a quid pro quo for DOJ's help with the Brand X case, or that both rulemakings (despite their heavily regulatory character) fit neatly into the apparent thematic thread of the current Republican White House by emphasizing security and law enforcement. It is more that both rulemaking efforts ignore major technical differences between the telephone system (centralized, controllable) and the internet (decentralized, any service can be added without permission), and attempt to apply telephony-based rules to the internet with almost no changes. This element of the E911 and CALEA rules, this failure to consider alternative ways of reaching desirable social goals, demonstrates the inexpert approach of the Commission to a world that has changed enormously. Expertise was not the basis of these rules. Indeed, it is easy to demonstrate better ways of reaching the FCC's social policy goals (see Part IV).

Just as expertise was not the basis for these rules, it would be impossible to say that they represent a "scientific" response to a political question. Instead, it is apparent that they are both deeply political responses to a series of political requests. Both rulemakings have at their heart important questions of social policy (how do we protect people? how do we help law enforcement to surveil people), which makes them difficult to attack. As a matter of both law and technical reality, however, they represent some of the most unlikely responses to these social questions.

For example, in the E911 world, who would have imagined that new VoIP services (capable of transmitting a picture of the house where the injury has occurred, able to gather health data and doctor contact data and convey it to emergency responders) would be required to use a 30-year-old

Era." Marc Allen Eisner, Regulatory Politics in Transition 48 (1993). The Progressives saw great value in independent regulatory commissions, as "an important conduit through which market correction was administered." Brefer at 1131. The idea of expert administrators with technical competence became very important during this era. Progressives believed in "the almost unlimited potential of science and administration." Brefer at 1131, citing Richard L. McCormick, The Party Period and Public Policy: American Politics from the Age of Jackson to the Progressive Era. The independent agency "was envisioned as an institution capable of compensating for the shortcomings of the 'political' institutions of American government." Eisner at 44. "Many believed that the only way to achieve effective business regulation was to establish a trade commission completely removed from the political fray." Brefer at 1132-33.

legacy system that sharply *limited* the emergency assistance they could provide? In the CALEA world, who would have imagined that the Commission would read the statute's exclusion of "information services" to allow *inclusion* of those services under the CALEA mandate? And who would have imagined that the online world, a great engine of economic growth in America, would have been subject to preapproval by law enforcement? This may sound (and possibly is) conclusory, but it is impossible to pretend that what the FCC did with the E911 and CALEA rules was apolitical. These were hardly "scientific" results.

Past chairs of the FCC understood very clearly that the FCC was a political entity.[232] And current Chairman Kevin Martin is undoubtedly a political actor. The chair of the FCC (as any independent agency) is the most powerful figure in the agency, is appointed by the President, and is part of his political party. Chairman Martin has close ties to the White House. Previous to his FCC job, he served on the Bush-Cheney transition team and was general council for Bush's 2000 Presidential campaign. His wife, Cathie Martin, is a former aide to Vice President Dick Cheney. She works in the White House as a special assistant to the President for economic policy.[233] The Martins are extremely well-connected to the White House, and Kevin Martin is very likely to be interested in ensuring that his agency is on the same page as the Administration.

C. Capture Theory

Absent some action by Congress, the FCC will continue to argue that it has broad delegated powers to regulate internet services. With this unlimited delegation and the FCC's broad preemption of any state efforts to make rules about online services,[234] capture is relatively easy: there is only one point to capture, and it is the FCC. This next subpart deals with the capture narrative that has resulted.

232. *See* Reed E. Hundt, You Say You Want a Revolution: A Story of Information Age Politics 19 (2000) ("Another revelation on day one was the omnipresence of congressional influence on the commission's work."). *See also id*. at 13 ("As a matter of law, the White House could not tell the FCC chairman or the commissioners how to vote. But naturally I, and any agency head, preferred the White House to approve of my agenda. Few are successful in any endeavor without learning the value of partnership. Moreover, the power of the White House to drive or block any agenda was, especially in the midst of the Gingrich Revolution, my primary source of support."). From Brefer & Edles, at 1137 n.127.

233. Associated Press, *Bush Names Kevin Martin New FCC Chairman*, Mar. 16, 2005.

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

1. Comparison of New Capture to Old Capture

The regulations at issue here do not fit the usual "capture" complaint, which focuses on agencies being captured by the very groups they are supposed to regulate. Although it is true that the Baby Bells were happy to visit regulatory burdens on their VoIP competitors, these case studies show that the FCC was captured in the E911 setting primarily by third-party middlemen—entities that are not regulated by the FCC. And the Commission, an independent agency,[235] was captured in the CALEA context by an executive agency—the Department of Justice. Neither of these stories is the traditional one.

From the first, the mere existence of administrative agencies has prompted questions as to their constitutionality and accountability.[236] But until relatively recently—the middle of the last century—few questioned that agencies were interested in serving the public good above all else. In the 1960s, however, federal judges became concerned about "capture."[237] The worry was that if agency officials were both given discretion to act and protected from political accountability, they would be subject to enormous pressures by the entities they regulated to help their particular business models rather than the public interest.[238] The term customarily used for this

235. The FCC has a bipartisan group of Commissioners who are appointed by the President with the advice and consent of the Senate and serve for five years. 47 U.S.C. § 154(a). The Telecommunications Act is silent concerning removal of Commissioners from office. The maximum number of Commissioners from any party is a number equal to the least number that would constitute a majority, and the Chairman serves as the Chief Executive Officer of the agency. The FCC is denominated as an independent agency. 44 U.S.C. Sec. 3502(5). For an extensive discussion of the practices of independent agencies, see Marshall J. Breger & Gary J. Edles, *Established by Practice: the Theory and Operation of Independent Federal Agencies*, 52 Admin. L. Rev. 1111 (2000).

236. Mark C. Niles, *On the Hijacking of Agencies (And Airplanes): The Federal Aviation Administration, "Agency Capture," and Airline Security*, 10 Am. U.J. Gender Soc. Pol'y & L. 381, 387 (2002) (analyzing allegation that FAA has been "captured") (noting that questions began with formation of Interstate Commerce Commission (abolished in 1995) in 1887). The idea of capture is generally assumed to stem from Marver H. Bernstein, REGULATING BUSINESS BY INDEPENDENT COMMISSION (1955).

237. *See* Thomas Merrill, *Capture Theory and the Courts*, 72 Chi-Kent L. Rev. 1039, 1042 (1997) (courts' assertiveness between 1967 and 1983 explained by concerns about capture and belief that courts could do something about it; replaced by later pervasive pessimism); Richard B. Stewart, *The Reformation of American Administrative Law*, 88 Harv. L. Rev. 1667, 1713 (1975) ("It has become widely accepted, not only by public interest lawyers, but by academic critics, legislators, judges, and even by some agency members, that the comparative overrepresentation of regulated or client interests in the process of agency decision results in a persistent policy bias in favor of these interests") (suggesting increase in judicial intervention and review). .

238. *See generally* Mark Seidenfeld, *A Civic Republican Justification for the Bureaucratic State*, 105 Harv. L. Rev. 1511, 1565-70 (1992) ("According to the capture hypothesis, instead of

problem is "pathology" – that agencies were subject to the pathologies of interest groups and regulated entities. The answer given by these 1960s-70s federal courts, at least initially, was that robust and energetic reform activities would fix the pathologies of agencies.[239] For example, famed D.C. Circuit Judge Skelly Wright demanded that the FCC put its ex parte contacts with industry on the public record, noting his concern "that the final shaping of the rules we are reviewing here may have been by compromise among contending industry forces, rather than by exercise of the independent discretion in the public interest the Communications Act vests in individual commissioners."[240] Expansion of citizens' standing rights and the "hard look" doctrine in the 1960s and 1970s can be understood as part of this robust reform approach aimed at reducing the risks of capture.[241]

In general, agency capture is said to happen when "compact groups whose members have high per capita stakes in a controversy out-organize and out-influence larger more diffuse groups."[242] Usually capture stories concern the excessive influence of regulated entities.[243] Thus, the academic

providing meaningful input into deliberation about the public interest, industry representatives co-opt government regulatory power in order to satisfy their private desires. Regulated entities are well organized and generally well funded, and they often have strong interests at stake, which they do not share with the polity as a whole. These entities have much to gain by ensuring that they have control over government decisionmakers and that the decisionmakers whom they do control remain in office."); John Shepard Wiley, Jr., *A Capture Theory of Antitrust Federalism*, 99 Harv. L. Rev. 713 (1986); Martin Shapiro, Who Guards the Guardians: Judicial Control of Administration 65-66 (discussing explanations of regulatory capture).

239. Merrill, supra n. 192, at 1052.

240. Home Box Office v. FCC, 567 F.2d 9 (D.C. Cir.), cert. denied, 434 U.S. 829, reh. denied, 434 U.S. 988 (1977). Wright ordered the Commission to submit a list of all ex parte communications, but fumed that "it is still not possible to determine the effect of such communications on the integrity of the rulemaking. As a result, the elaborate public discussion in the dockets here under review may be a sham and a fiction." Id. at 15; cf Action for Children's Television v. FCC, 564 F.2d 458 (D.C. Cir. 1977) (ex parte prohibitions in rule-making proceedings only applicable when competing private claims to a valuable privilege involved).. In Home Box Office, Skelly Wright ordered that the substance of all ex parte conversations be written down and filed. Id. It is fair to say that the Intrado and Level 3 filings do not reveal much of the substance of the conversations they record. It is also fair to say that there were undoubtedly many DOJ contacts that were never reflected in public filings.

241. David B. Spence, *A Public Choice Progressivism, Continued*, 87 Cornell L. Rev. 397, 410 (2002) (sketching history of Progressive movement and capture response).

242. Merrill at 1053. In an important paper, George Stigler developed the "capture theory," suggesting that "regulation is acquired by the industry and is designed and operated primarily for its benefit." George J. Stigler, The Theory of Economic Regulation, 2 Bell J. Econ. & Mgmt. Sci. 3, 3 (1971).

243. "In 'captured' agencies, agency regulators do not act as 'arms-length' representatives of some larger ';public interest' in their interaction with regulated industries. Instead, government

literature contains accounts of the alleged capture of the FAA by the airline industry,[244] the capture of the USDA by the meat and poultry industries,[245] and the capture of the Nuclear Power Agency by power plants.[246] In all of these cases, the agency is said to have lost focus on its public mission in favor of the interests of regulated private actors.

Capture theory is often criticized as imprecise and over-simplified,[247] both because it is difficult to say when private interests fail to coincide with the overall public interest, and because it deals insufficiently with the messy world of real politics. It is, for example, often true that agencies have to depend on outside sources of information. It is also true that organized interests, like regulated firms, often provide that information. They have non-corrupt reasons to do so, for they have a stake in the policy that will emerge and the resources to help.[248] By contrast, consumers and other unorganized interests ordinarily have stakes that are too small to justify intervening in the agency's work. There is nothing necessarily wrong with this reality.

Capture theory has been gradually subsumed by increasingly pessimistic public choice theory, under which all governmental decisions are seen as the result of rent-seeking behavior on the part of many different groups.[249] Very roughly speaking, "[m]odern public choice theory regards

officials work to advance the agenda of current firms in the industry by formulating regulations that benefit or at least do not substantially burden the industry." David Dana & Susan Koniak, *Bargaining in the Shadow of Democracy*, 148 U.Pa. L. Rev. 473, 497 (1999) (exploring "regulatory contract" phenomenon). "According to the capture hypothesis, instead of providing meaningful input into deliberation about the public interest, industry representatives co-opt government regulatory power in order to satisfy their private desires. Regulated entities are well organized and generally well funded, and they often have strong interests at stake, which they do not share with the polity as a whole. These entities have much to gain by ensuring that they have control over government decisionmakers and that the decisionmakers whom they do control remain in office." Mark Seidenfeld, *A Civic Republican Justification for the Bureaucratic State*, 105 Harv. L. Rev. 1511, 1565-70 (1992).

244. AmUJGender at 401.

245. Dion Casey, Agency Capture: The USDA's Struggle to Pass Food Safety Regulations, 7 Kan. J. L. & Pub. Pol'y 142 (1998).

246. Seidenfeld, 464-65.

247. Dana at 497. "[I]t is possible to speak of illegitimate interest group influence only if one has a coherent normative baseline defining legitimate interest group influence."

248. See Richard B. Stewart, *The Discontents of Legalism: Interest Group Relations in Administrative Regulation*, 1985 Wis. L. Rev. 655, 663-65 (constructive relationships between regulators and regulated industry can benefit society, avoid litigation, and do not represent capture).

249. *See*, *e.g.*, Farber & Frickey, The Jurisprudence of Public Choice, 65 Tex. L. Rev. 873, 883-906 (1987). Roughly, public choice is the "application of the economist's methods to the political scientist's subject." Daniel A. Farber & Philip P. Frickey, Law and Public Choice 1

all organized groups demanding services from political institutions--including not just business and producer groups, but also environmental groups, labor unions, civil rights groups, and rent control activists--as being subject to a unitary logic of collective action."[250] Unlike the capture theorists who suggested reforms of agency processes to protect against capture, early public choice theorists did not necessarily propose a path forward; rather, they aimed to demonstrate that regulatory decisions were inherently biased, and that market-mimicking agency actions should usefully be replaced by markets themselves or never delegated in the first place.[251] Early on in public choice scholarship history, reform efforts became seen as impossible, and the simple libertarian response was to pull up stakes and remove discretion from administrative agencies.

In the present day, the delegation debate continues, unabated. The enormous world of public choice scholarship has become a rich one that is no longer simply based on seeing venal motives in every step by a regulator. Today, "public choice" can mean anything from modeling complex systems inside agency decisionmaking to empirically examining influence across a wide range of decisions by a wide range of institutional actors.

My contribution to the enormous capture/public choice literature is modest. I am providing a live case study showing that prior capture theories may have been too simple in their focus on regulated firms.[252]

(1991). *See also* Daniel A. Farber & Philip P. Frickey, Foreword: Positive Political Theory in the Nineties, 80 Geo. L.J. 457 (1992) (defining public choice as using economics to focus on the maximizing behavior of rational beings). Not all administrative law scholars accept the "homo economicus" view that public choice theorists posit. Abner J. Mikva, *Foreword*, 74 Va. L. Rev. 167, 168 (1988) (condemning view of human nature fostered by public choice analyses).

250. Merrill, supra n. ___, at 1069; see also Jody Freeman, *The Private Role in Public Governance*, 75 N.Y.U. L. Rev. 543, 561 (2000) ("Public choice theory understands administrative decision as the product of interest group pressure brought to bear on bureaucrats seeking rewards such as job security, enhanced authority, or the favor of powerful legislators upon whom the agency depends...treating agency outcomes as products of interest group appeals to individual bureaucrats' preferences.")

251. David B. Spence & Frank Cross, A Public Choice Case for the Administrative State, 89 Geo. L.J. 97, 98-99 (2000) (citing scholars who feel public choice is hostile to delegation).

252. I am not the first to discover that nonregulated private firms may have captured an agency's decision making. In a 1993 article, Bradford Mank suggested that contractors hired by EPA to conduct Superfund cleanup activities had formed a "dependent bureaucracy that fed on the program's structural incentives," a conclusion that had earlier been reached by the congressional Office of Technology Assessment. Bradford C. Mank, *Superfund Contractors and Agency Capture*, 2 N.Y.U. Envtl. L.J. 34, 60-63 (1993). Mank noted that James Q. Wilson had argued that nonregulated interest groups develop "client relationships" with agencies. Mank at 51, citing James Q. Wilson, Bureaucracy: What Government Agencies Do and Why They Do It

Here, the capturing interests were neither regulated entities nor, in the case of the E911 rule, particularly visible. But both law enforcement and E911 outsourced services firms are intensely concentrated interests (as opposed to diversified public interests) that can claim expertise and devote resources to push for their version of regulation. And both likely received better treatment from the FCC in these rules than they could have gotten from Congress. My assertion is that, in both the E911 and CALEA contexts, rules were written that benefited an identifiably smaller "public" interest at the expense of a larger, but more diffuse, one: the interest in continued online innovation.

In the E911 context, a largely invisible vendor, making opaque "ex parte" filings, was able to have a rule put in place that assured its continued dominance and relevance. Without even giving VoIP providers the time to show that alternative E911 schemes could have provided better (more modern, more informative) results for consumers, the Commission forced them to interconnect with hardware controlled almost completely by that invisible vendor, at a cost that vendor could control. Failure to connect in this fashion will lead to the risk of having to cut off their customers, and has led to unprecedented marketing constraints being established by the Commission.

In the CALEA context, an interest group in the form of another sister agency, the Department of Justice, was able to obtain rules that it likely could not have gotten from Congress. It is likely that there were broad ex parte contacts between DOJ and FCC before DOJ sought a petition for certiorari in the Brand X case.[253] (Because these contacts would have been related to ongoing litigation rather than an open rulemaking, nothing would have been made public about them.) The DOJ was even able to have the FCC set a hard 18-month deadline for compliance without any indication of what compliance meant. And, as in the E911 context, innovation is very likely to suffer: law enforcement appears to be seeking pre-launch approval of any potentially covered application or connection, to ensure that desired data fields are available to them.

Where an agency is in thrall to a sister agency, and that sister agency

74-88 (1990) (discussing academic scientists' relationship with the National Academy of Sciences and National Science Foundation). Mank suggested limiting contractor functions and strengthening EPA enforcement efforts. Id. at 76-77.

253. "A reliance on impermissible factors renders an agency decision arbitrary." Brefer, 1193, citing Motor Vehicle Mfrs. Ass'n v. State Farm Mut. Aut. Ins. Co., 463 U.S. 29, 46 (1983) (concluding agency's decision to rescind rule was arbitrary and capricious).

is asserting itself as a single, governmental audience for a standard that will have dramatic effects on innovation, neither traditional "capture" nor more recent "public choice" theory fits the situation. Traditional capture theory never envisioned that the capturer would be another government agency. Rather, the enemies of the public interest were viewed as business interests, with unions and civil society viewed tacitly as carrying out the public interest themselves in their interactions with agencies. Under capture theory, a sister agency would certainly have been viewed as having the public interest at heart, and no "fixes" would have been called for. As for public choice theory, there is no market-mimicking behavior being approximated by the FCC; indeed, because there is no competition for the government's desire for information, no "market" forces can possibly operate to set the scope of coverage and level of compliance. So public choice criticism will not help; there is no "market" to which to devolve the creation of the standard.

2. The Limits of Traditional Answers to Capture

The traditional answer to capture problems has been procedural. For example, Judge Skelly Wright in *Home Box Office*[254] thought that having ex parte filings put on the record might help. But in this setting, even had there been more information about the respective roles of third party vendors or law enforcement, there are no other actors involved that have the resources and concentrated attention to act on these disclosures. The internet is useful in spreading information about what is going on at the FCC, but it cannot embarrass the FCC out of this kind of action; the FCC sees itself as simply having been convinced by the most forcefully and articulately (and expertly) advanced set of considerations about technical matters. Additionally, the leader of the FCC will certainly not be embarrassed about forwarding his Administration's objectives.

Similarly, strengthening "revolving door" prohibitions (keeping former staffers from lobbying their agency for a longer period of time) are unlikely to help. The problems in these rulemakings are not a matter of corruption or of individual agency actors seeking personal advantage. The problems stem from an absence of organizational structures that have the resources and incentives to fight for the public good when that good is innovation. Thus, even if sunlight and non-corruption rules might help

254. Home Box Office, Inc. v. FCC, 567 F.2d 9 (D.C. Cir.) (per curiam), cert. denied, 434 U.S. 829 (1977).

prevent capture by the regulated industry itself, there will still be capture by the potential beneficiaries of a central rule—even when those beneficiaries are other arms of government or vendors who can help industry comply with the rule.

IV. BETTER WAYS FORWARD

Many inextricably intertwined factors have led the FCC to assert "social policy" control over internet services without translating those policies for the internet age. Commission staff members, although operating with the best will in the world, may have been blinded by their telephony mindsets to the implications of the Commission's current trajectory. Capture by third party vendors and law enforcement may have been difficult to avoid, given the intensity of their involvement and their superior technical resources. And lobbying efforts by current (old-style) communications providers have been extraordinary: between 1998 and 2004, the communications industry as a whole (including broadcast) spent $1.1 billion to affect the work of the Commission and Congress, and the cable and telephone industries alone spent $100 million in 2004.[255] (By contrast, the oil and gas industry spent $396 million between 1998 and 2004 on lobbying.)[256] Since 1997, almost 400 FCC staff and congressional employees have gone to work in the communications industry.[257] Both the communications industry and law enforcement authorities have great influence with key FCC staff. At the same time, the FCC's internal resources are constrained.[258]

Thus, the only institution that can help here is Congress. Because there are so many more players who can intervene in any given legislative matter, and so many more independent leaders who can have a point of view, it takes much less force to block something in Congress than at the FCC. Congress, unlike the FCC, has no institutional imperative to come up with a particular solution that will make either incumbent telephone

255. Center for Public Integrity study, *Networks of Influence: The Political Power of the Communications Industry*, Oct. 28, 2004, *available at* http://www.publicintegrity.org/telecom/report.aspx?aid=405). [The cable TV industry has spent $37.4 million on federal political contributions since 1990, says the Center for Responsive Politics. That's dwarfed by the $102 million doled out by phone companies in that period.] Investor's Business Daily, 10/19/05.

256. *Id*.

257. *Id*.

258. In 1999, the FCC established a Technical Advisory Committee to assist it with questions requiring technical expertise. Press Release, Federal Communications Commission, FCC Announces Formation of Technological Advisory Council, Apr. 1999.

companies or law enforcement happy. Indeed, if Congress had decided, in advance, that we needed a single rule for both E911 and CALEA (something it decidedly did not do), it would have in effect licensed capture of the political process by whoever had the interests that are most concentrated and motivating. Because Congress arguably did not make such a delegation, we can consider afresh whether a delegation of the powers the FCC asserted in the E911 and CALEA Orders is necessary.

Provision of emergency services and assistance to law enforcement have in the past been deemed by Congress to be worthy social goals for telephony.[259] Now that more of life is migrating online, a decision needs to be made as to whether these same social goals are appropriate for the internet. As discussed above, the FCC has asserted power to implement these social goals online through regulatory back doors based on either its very broad understanding of its implicit "ancillary" powers under the Telecommunications Act or a willful misreading of CALEA. The Commission is no doubt straying beyond its statutory powers, and the lawsuits that have been filed are likely to be successful. In order to avoid the capture that has been described in this Article, Congress should decide what list of social policies is the right one for the internet, and how any such policies should be implemented in the online environment.[260]

If we assume that emergency service support should continue to be relevant for phones, that consumers will continue to expect that 911 will function for phones, and that it should not matter whether the phone uses circuit-switched or packet-switched technologies, Congress needs to work on the question of "what is a phone." Perhaps only those things that *are* identified as phones (in special colors, marked PHONE, using traditional handsets) should be mandated to have E911 service that connects to a central selective router. Through public service campaigns and other marketing efforts, Congress could make very clear that the thing that is a PHONE has 911 access, and PHONES could provide quite elaborate and innovative services on top of merely giving access to location information. This would not preclude other applications, other things that are not PHONES, from having extensive safety features as a voluntary matter. This focus defining PHONES would serve consumer expectations, but

259. *See* 47 U.S.C. §§ 228, 229, 254, 255, 258 (2000) (CALEA, universal service, access for persons with disabilities and anti-slamming).

260. Congress should also consider exercising its authority to circumscribe what administrative remedies may be called for by the Agency, and should state clearly where the Agency's authority begins and ends.

would keep new technologies from being forced to use a broken legacy system. Doors that held conversations with you would not be PHONES.

As for CALEA, it is not clear why law enforcement should be entitled to an amendment to that law that would cover what they obtained through the FCC's good offices. Congress should, at the most, bless law enforcement's ability to, with proper legal authorization, gain access to streams of information that they must parse to obtain what they are authorized to read. There is no good policy reason to make all VoIP applications have to be approved in advance by law enforcement. First, the costs of such a step far outweigh any possible benefits. Second, there is no principled line between VoIP applications and any other online application, because a bit is a bit. Congress should state clearly that CALEA is for PHONES. Taking the route requested by law enforcement of extending CALEA to "interconnected VoIP" and broadband access will lead to another outsourced vendor capture problem when VeriSign claims it can assist all possible actors with compliance. On a meta level, it is clear that law enforcement believes it has authority to, Carnivore-like, inhale all possible data and parse it.[261] If it can do that, surely it does not need applications to be designed in advance so as to be easily tappable.

There are better, more internet-minded ways to get law enforcement the information it wants pursuant to lawful wiretap orders. Rather than requiring centralized, FBI approval of the design of all online applications prior to launch to ensure that they are easy to tap (something of which a telephony-minded person would instinctively approve), ISPs could make streams of data available that could be accessed by law enforcement only following issuance of a subpoena or other judicial order.[262] Rather than forcing the standardization of data, law enforcement could learn how to understand traffic associated with particular people—already located by ISPs for them—once a subpoena has issued. It may be better to trust law enforcement to restrain itself in accessing data at the edge of the network rather than to force innovators to enter into negotiations with centralized law enforcement authorities over the development of new online services.

261. Eric Lichtblau & James Risen, *Spy Agency Mined Vast Data Trove, Officials Report*, New York Times, Dec. 24, 2005 (National Security Agency traced, analyzed large volumes of telephone and internet communications flowing into and out of the United States as part of the eavesdropping program that President Bush approved).

262. Indeed, DOJ has said that it is interested in having all ISPs store information for its use, and it is more than conceivable that the FCC could use its newly-enhanced "ancillary jurisdiction" over ISPs (discussed in Section D, *infra*) to ensure that this happens. Declan McCullagh, *Your ISP As Net Watchdog*, CNET NEWS.COM, Jun. 16, 2005, *available at* http://news.com.com/Your+ISP+as+Net+watchdog/2100-1028_3-5748649.html.

Law enforcement's appetite for data is insatiable, and we will need to find some internet-minded way of responding to their requests that balances respect for the rule of law with concerns about innovation. The internet, after all, provides law enforcement with potentially better, more detailed, and more quickly-available information than it could ever have obtained offline. But law enforcement is causing the FCC to apply telephony-world rules and assumptions to a changed IP world, with no regard to the consequences.

CONCLUSION

The E911 and CALEA rulemakings show that it is inappropriate to allow a toxic combination of broad, unquestioned delegation, lack of political accountability, resulting capture by concentrated interests (vendors or law enforcement), and bogus claims of "expertise" to create a single rule about how intangible online services may be offered. It is far too easy for old technology players, some of them invisible, to take over the rulemaking process at the FCC.

These are just the first two rulemakings. There will undoubtedly be many more, and they will likely have similar effects on innovation and the national economy. FCC regulation of the internet is just emerging, and governments all around the world are following suit. Thus, the U.S. has an opportunity to take the lead in self-restraint, but Congress will need to be thoughtful and acknowledge the differences between telephony and the internet—something it seems often to have trouble doing. There is very little information available to policymakers about how treating the internet as a telephone network will affect our future. There is ample latitude for work on why (or whether) adopting an internet mindset—encouraging decentralized, alternative ways to reach agreed social goals—will provide a more encouraging framework for economic development. We have time to consider the potential troubles that will be created if this kind of alternative approach is adopted. The first step should be for Congress to reexamine the enormous power the FCC is asserting over all possible online activities. We should not risk our collective online future by continuing to stumble forward as we have thus far.

For online companies, the need to step up as policy players and lead the public along a new trajectory poses an enormous challenge. Very few companies seem to be willing to take on the FCC's appetite for internet

regulation, for fear of being branded anti-law enforcement, anti-consumer, pro-pornography, or some other headline-grabbing attribute. But the short-term attractiveness of making deals with cable and telephone companies should be far outweighed by the attractiveness of the internet's future.

The FCC needs to recognize that it has in many senses been captured by its own history. It should not pretend to be "the internet agency," and it does not have the capacity to draw lines that will make sense in this quickly-evolving set of circumstances. Indeed, no one does. Technical mandates and requirements based on legacy understandings and technologies (like the E911 fiasco) are doomed to be unsuccessful and to serve only the incumbents and outsourced compliance vendors who demanded them in the first place. The regulators need to take the time to evaluate, within the sharply-defined mandate handed them by Congress, how to address the social policies in which they are interested. It may be that a single rule is always inappropriate for the online world.

The great advantage of understanding how the internet works is that this network of networks finally makes possible the kind of collaboration and self-determination that is the stuff of human dreams. The internet encourages economic development and human empowerment on many levels. To cut off all of these benefits in favor of today's focus on "security" or "safety" would be unfortunate and wholly short-sighted. In an increasingly flat world, U.S. users of the internet gain few benefits from the kinds of regulatory activities described in this Article, and the sooner we recognize this in policy as well as in reality the better off will be the U.S. economy.

That a crucial set of misunderstandings, pathologies, and incorrect assumptions has led us down a destructive path does not mean that we should not make an effort to correct them. Awareness of the trajectory currently being followed (largely unnoticed) by the FCC presents a fascinating opportunity that could allow us, as a nation, to lead the world in encouraging enormous innovation, creative growth, and human collaboration. It is essential that we try.