A MODEL FOR EMERGENCY SERVICE OF VOIP THROUGH CERTIFICATION AND LABELING

Tom Lookabaugh
Patrick S. Ryan
Douglas C. Sicker*

---

* Tom Lookabaugh, PhD (Stanford), is an Assistant Professor of Computer Science at the University of Colorado at Boulder and Faculty Director of the Interdisciplinary Telecommunications Program. His bio is *available at* http://tinyurl.com/3tcfx. Patrick S. Ryan, PhD (Leuven), JD (Texas), is an Adjunct Professor at the University of Colorado School of Law, a faculty member of the Interdisciplinary Telecommunications Program, a Guest Professor at the Katholieke Universiteit Leuven, and a practicing lawyer. His bio is *available at* http://tinyurl.com/58vvg. The primary author of this piece is Douglas Sicker, PhD (Pittsburgh), an Assistant Professor of Computer Science with a joint appointment in the Interdisciplinary Telecommunications Program. His bio is *available at* http://tinyurl.com/59tyf. The authors are grateful to many people for comments and advice, including Hary Balasubramanian, Carolyn Daughters, Raunaq Gahndi, and Wendy McCallum, and Ron Rehling.

ABSTRACT

Voice over Internet Protocol (VoIP) will transform many aspects of traditional telephony service, including the technology, the business models, and the regulatory constructs that govern such service. Perhaps not unexpectedly, this transformation is generating a host of technical, business, social, and policy problems. In attempting to respond to these problems, the Federal Communications Commission (FCC) could mandate obligations or specific solutions to VoIP policy issues; however, it is instead looking first to industry initiatives focused on the key functionality that users have come to expect of telecommunications services. High among this list of desired functionality is user access to emergency services for purposes of summoning fire, medical, and law enforcement agencies. Such services were traditionally required to be implemented (and subsequently were implemented) through state and federal regulations.

An emergency service capability is a critical social concern, making it particularly important for the industry to propose viable solutions for promoting VoIP emergency services before regulators are compelled to mandate a solution. Reproducing emergency services in the VoIP space has proven to be a considerable task, mainly due to the wide and diverse variety of VoIP implementations and implementers. While technical and business communities have, in fact, made considerable progress in this area, significant uncertainty and deployment problems still exist.

The question we ask is this: Can an industry-based certification and labeling process credibly address social and policy expectations regarding emergency services and VoIP, thus avoiding the need for government regulation at this critical time?[1] We hypothesize that the answer is "yes." In answering this question, we developed a model for VoIP emergency service compliance through industry certification and device labeling. This model is intended to support a wide range of emergency service implementations while providing users with sufficient verification that the service will operate as anticipated. To this end, we first examine possible technical implementations for VoIP emergency services.[2] Next, we summarize the theory of certification as self-regulation and examine several relevant examples. Finally, we synthesize a specific model for certification

[1] We would like to acknowledge and thank the NET Institute (http://www.NETinst.org) for supporting this project.

[2] Note that we use the term "emergency services" for VoIP rather than specifying it as E911 for VoIP. We make this distinction in order to distinguish between the technology of traditional emergency services carried over the Public Switched Telephone Network (PSTN) versus those services carried over IP and to emphasize that emergency services in the IP space might be very different from traditional E911 in terms of function.

of VoIP emergency services. We believe that the model we describe provides both short-term and long-term opportunities. In the short term, an industry-driven effort to solve the current problem of VoIP emergency services, if properly structured and overseen as we suggest, should be both effective and efficient. In the long term, such a process can serve as a self-regulatory model that can be applied to social policy goals in the telecommunications industry, making it an important tool to have as the industry becomes increasingly diverse and heterogeneous.

I. Introduction

VoIP promises to upend a century-old model of voice telephony by creating a more dynamic marketplace and by changing the point of control from the central office switch to the end user's device. The transformation to VoIP is only in its very early stages, and it will ultimately impact all sectors of the telecommunications services industry, including traditional incumbent local exchange carriers, cable providers, wireless service providers, and emergency service providers. In fact, all of the relevant stakeholders affected by VoIP (*e.g.*, service providers, hardware and software vendors, customers, and governmental agencies) share a great need to analyze the issues raised by the transition from the traditional Public Switched Telephone Network (PSTN) to a packet-switched, Internet Protocol (IP)-based architecture. For example, service providers and hardware and software developers are struggling to understand and take advantage of opportunities in this area involving new technology prospects (*e.g.*, integrated messaging and mobile collaboration). Moreover, business, governmental, and residential consumer users of telecommunications equipment and services are seeking guidance on when and how to upgrade to a new technological frontier. Finally, governmental agencies are struggling to ensure that social policy concerns will be addressed in this very different technological environment.

The social policy implications of VoIP present regulators and incumbent businesses with an unusual dilemma, forcing them to choose from amongst mutually exclusive—and equally unfavorable—options. Under the current PSTN-based voice telephone network, many critical policy goals, such as the provision of reliable emergency services, are implemented effectively and reliably. However, most VoIP services, at least as they exist today, do not deliver the same level of quality and dependability as emergency services. In response, some state regulators have considered passing regulations requiring VoIP to meet legacy (and other) requirements, regardless of the dramatic differences in the VoIP services technical and business models.[3] The FCC has only begun to develop its regulatory VoIP strategy, although former Chairman Michael Powell had made it clear that the strategy would need to differ from the legacy model used in the PSTN context, a position likely to continue in successor FCC administrations.[4] With these thoughts in mind, it is unclear how VoIP services might evolve in a meaningful and timely fashion.

In a number of specific circumstances, however, self-regulation can be a viable alternative to government regulation. Certification, in particular, can be provided by a self-regulatory body as evidence of conformance to required attributes, practices, or policies. Self-regulation has a number of potential advantages, and in the case of VoIP emergency services we are particularly interested in recognizing information asymmetries between industry and government, given the increase in complexity and heterogeneity inherent in the move from PSTN to VoIP. In order for self-regulation to be viewed as a credible alternative and in order for it to ultimately succeed, it needs to be situated within a careful institutional framework that includes (1) a clear and consistent external motivation (*e.g.,* an incentive in terms of third-party liability), (2) a process for determining the specifications to be certified, (3) identification of certifiers and determination if a competitive market for certification exists, (4) reference to an appropriately neutral accrediting party (a role that government can but does not have to fill), (5) communication of certification to users, and (6) policing of certification. The telecommunications industry has repeatedly demonstrated the ability to self-regulate in areas of interoperability where economic motivation can be relied on to incentivize the activity. In this case, though, we propose that the industry self-regulate in order to address a social policy goal. Success in this area could even help self-regulation become a tool that could be applied in other areas of social policy (especially in the development of new policy initiatives that would otherwise be imposed through government regulation of telecommunications, as has traditionally been the case).

The particular technical challenges surrounding VoIP emergency services arise from two major drivers: variability and location. VoIP can be

---

[3] *Vonage Holdings Corp. v. Minn. Pub. Utils. Comm'n,* 290 F. Supp. 2d 993 (D. Minn. 2003). Note that newer service providers have already started to tell consumers that VoIP services may not meet traditional E911 expectations, although they have not yet described what the alternative expectations might be. For example, an AT&T spokesperson, referring to the company's consumer VoIP service, indicates, "We make very clear to our customers that our CallVantage Internet phone service does not work the same as traditional landline 911." *911 Calls Made Over Internet Often Get Lower Priority*, USA TODAY, October 12, 2004, *available at* http://www.usatoday.com/tech/news/2004-10-12-voip-trouble_x.htm.

[4] Written statement of Michael K. Powell on Voice over Internet Protocol (VoIP), February 24, 2004, *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-244231A1.pdf.

seen as a much more variable service than traditional PSTN-based telephony, and many new business models and technical combinations are emerging in which quality, methods of initiating and terminating calls, integration with other messaging technologies,[5] and types of terminals (*e.g.*, phones, PDAs, and PCs) have all become heterogeneous. For emergency services in particular, IP networks are fundamentally location independent, and VoIP services may run on IP networks over many different types of wired and wireless access.[6] As a result, these realities challenge a fundamental modern expectation—that an emergency services dispatcher can identify the caller's location even if the caller does not know the location or is not able to describe it. Although substantial technical progress is being made regarding the provision of emergency services in various VoIP settings, users may not be able to determine prior to an emergency whether the particular service they are employing is emergency service capable. Accordingly, we propose to use labeling as a means of specifying the particular level of emergency service capability provided, in recognition of the fact that VoIP's diversity will preclude a single common requirement for all possible VoIP services. We also propose that an emergency service testing capability be made available to the end user.

In this paper, we will describe the technical issues surrounding emergency service in VoIP, examine the status of proposed technical strategies,[7] and identify candidate criteria to be used in certification. Furthermore, we will examine the theories behind and examples of successful certification within self-regulatory regimes, including (1) the use of certification in product safety, (2) the use of certification in particular by Underwriters Laboratories acting as certifying institutions, (3) ISO 9000 quality system certification, (4) interoperability certification within the telecommunications industry through Cable Television Laboratories and

---

[5] Indeed, we should ask to what extent social policy expectations of emergency services response to voice communications should also apply to the many other modes of communication that are now popular or that may become popular, such as email, instant messaging, and video telephony. Given the possible breadth of regulation implied by such an increase in scope, we submit that the option of effective self-regulation would be even more valuable for all of these services than for telephony emergency services alone.

[6] For example, VoIP is increasingly carried over Wi-Fi wireless local access networks, and dual-mode phones that can switch between VoIP/Wi-Fi and cellular service are now being marketed. *See* Corie Lok, *One Person, One Phone*, TECH. REV., March 2004, *available at* http://www.technologyreview.com/articles/print_version/innovation10304.asp, and Marguerite Reardon, *Wi-Fi and VoIP: Is Sum Greater Than Parts,* CNET.COM, March 1, 2004, *available at* http://news.com.com/2102-7352_3-5167782.html.

[7] VoIP has a number of different signaling frameworks, including the Session Initiation Protocol (SIP) and H.323. For the most part, we attempt to proceed in a framework-independent manner in this paper; however, in cases where the framework is relevant, we focus on the SIP framework. We fully acknowledge that development of actual certification standards will need to consider multiple frameworks. Our emphasis on SIP is motivated by technical, market, and policy issues that are outside the scope of this paper. *See* Glenn Fleishman, *An Internet Extension to Your Telephone Twin*, N.Y. TIMES, August 28, 2003, at G3 (explaining in basic terms how a SIP phone works). For a good overview of SIP, *see generally* the SIP Working Group homepage on the Internet Engineering Task Force website, *available at* http://www.ietf.org/html.charters/sip-charter.html.

Telcordia, (5) the Wi-Fi Alliance as a consumer-oriented certification consortium, and (6) general experience with self-regulation in environmental policy. In the end, we will synthesize these insights in order to propose specific recommendations on institutional design, technical criteria, and the certification process.

II. EXISTING MODELS FOR CERTIFICATION

In this section, we will share the results of secondary research into existing certification processes. Drawing on historical analysis and literature review techniques, this research incorporates the collection and analysis of original descriptions, outcomes research on certification processes, and research on the manner in which these processes have been embedded in overall policy systems including government regulation. In the end, we will offer an overall model for successful certification tailored to the particular technical and industrial circumstances of VoIP.

A. Theory and Practice of Certification

Well-established certification processes are used in professions such as medicine and law to accredit practitioners, in securities markets by underwriters and auditors, and in product safety and compatibility arenas. More recently, certification and, more broadly, self-regulation have emerged in new social policy settings (*e.g.*, the certification of a manufacturer's compliance with labor practice expectations in developing countries or with specific environmental practices). Substantial research has created a reasonable understanding of the purpose of certification, as well as of its challenges and drawbacks.

Certification can have both economic and social policy goals. In economic terms, products or services may have attributes (such as quality or safeness) that buyers have difficulty ascertaining prior to the purchase. As a result, consumers oftentimes cannot distinguish between products, a situation that leaves little incentive for companies to include the attributes in the first place. Although reputation (brand) and warranties may mitigate this effect, such factors fall short if they are inconsistent or if customers find it too difficult or costly to apply the factors as a recourse. Certification can thus provide an alternate method for reliably signaling attribute distinctions.[8] For social policy, certification (as an aspect of self-regulation) can serve as an alternative or complement to government regulation. In

[8] Gian Luigi Albano & Alessandro Lizzeri, *Strategic Certification and Provision of Quality,* 42 INT'L ECON. REV. 1, 267-283 (2001).

other words, certification can be used as a means of avoiding the overproduction of negative social externalities (*e.g.,* pollution) and the underproduction of positive social externalities (*e.g.,* safety policies).

Moreover, certification can offer important advantages over direct "command-and-control" regulation. For example, certification can reduce the demand on government services and, consequently, on required levels of taxation (or, put another way, certification can better accommodate a neo-liberal reduced-government capability). It can also exploit information asymmetries in which industry participants have more (and better) information than a potential government regulator.[9] The direct use of industry information may increase the rate at which regulation can adapt as circumstances change and may also subsequently reduce the need to enumerate all conceivable contingencies, resulting in more flexible and lighter-weight regulation.[10] Furthermore, preemptive self-regulation may eliminate the need for industries and their opponents to make politically motivated investments in regulatory policies.[11]

Self-regulation can also have a moral and cultural effect by inculcating an ethical component in institutional self-image that induces behavior that exceeds mere compliance with the letter of the law.[12] Conversely, imposition of rigid regulation instead of self-regulation on sectors that have a strong anti-authoritarian tradition can, as commentator Darren Sinclair notes, "destroy virtue in the business community."[13] We believe that it is far too early to suggest that the telecommunications industry is incapable of producing its own solutions.

---

[9] Hayne E. Leland, *Quacks, Lemons, and Licensing: A Theory of Minimum Quality Standards*, 87 J. POLITICAL ECONOMY 6, 1328-1346 (1979) [hereinafter: Leland, Quacks, Lemons, and Licensing].

[10] Christodoulos Stefanadis, *Self-Regulation, Innovation, and the Financial Industry*, 23 J. REG. ECON. 1, 5-25 (2003).

[11] In this case, the end result is a Pareto improvement in welfare. *See* John W. Maxwell, Thomas P. Lyon, & Steven C. Hackett, *Self-Regulation and Social Welfare: The Political Economy of Corporate Environmentalism,* 43 J. LAW & ECON. 583 (2000) [hereinafter: Maxwell, *et. al.*, Self-Regulation and Social Welfare]. *Also see* THE ECONOMIST'S Research Tools, *available at* http://www.economist.com/research/Economics/, which defines Pareto efficiency as follows:

> A situation in which nobody can be made better off without making somebody else worse off. Named after Vilfredo Pareto (1843–1923), an Italian economist. If an economy's resources are being used inefficiently, it ought to be possible to make somebody better off without anybody else becoming worse off. In reality, change often produces losers as well as winners. Pareto efficiency does not help judge whether this sort of change is economically good or bad.

[12] Marius Aalders & Ton Wilthagen, *Moving Beyond Command-and-Control: Reflexivity in the Regulation of Occupational Safety and Health and the Environment*, 19 LAW & POL'Y 4, 415-443 (1997), and Simon Ashby, Swee-Hoon Chuah, & Robert Hoffmann, *Industry Self-Regulation: A Game-Theoretic Typology of Strategic Voluntary Compliance*, 11 INT'L J. OF THE ECONOMICS OF BUS. 1, 91-106 (2004) [hereinafter: Ashby, *et. al.*, Industry Self-Regulation].

[13] Darren Sinclair, *Self-Regulation Versus Command and Control? Beyond False Dichotomies*, 19 LAW & POL'Y 4, 529-559 (1997) [hereinafter: Sinclair, Self-Regulation Versus Command and Control].

On the other hand, certification can have undesirable side effects that should be anticipated in institutional design. If certifiers are under the control of the body being certified, certification may be deliberately structured to restrict new entrants and extract monopoly rents for already certified parties,[14] an attribute of guilds that continues in contemporary professions that require certification.[15] A parallel social policy concern relates to the credibility of the certifier, who may be perceived as being too tightly controlled by the certifying body.[16]

Ironically, though, should certification preempt some other form of regulation and succeed in spurring innovation and even new entrants, it is quite possible that incumbents would view the previous form of regulation as preferable even though a broader social perspective would favor certification. For this reason, we cannot conclude with assurance that all industry players will prefer certification even if it benefits both industry as a whole and society at large.

If the certification capability is limited to a single or small number of suppliers of certifications, the certification process itself might capture monopoly rents to the detriment of suppliers or consumers. More generally, even a competitive certifier market can exhibit peculiarities depending on the level of certifier liability, the regulation of the certifier market, and the amount of competition[17] (*e.g.*, situations in which certifiers do not provide all information or choose to provide noisy information).[18] The structure of the certifier market is consequently a non-trivial consideration.

[14] *Id.*, at 38. Leland provides a more nuanced analysis of whether licensing results in standards that are too high in order to restrict competition: "If a professional group or industry is allowed to set minimum quality standards (self-regulation), these standards may be set too high or too low. On balance, however, there is some reason to expect too-high standards will be the more likely case." Leland, Quacks, Lemons and Licensing, cited *supra* at note 9, at 1342. *See also* Ulrike Schaede, *Industry Rules: From Deregulation to Self-Regulation,* 28 THE JAPANESE ECONOMY 6, 35-58 (2000). Schaede points out a related problem in which apparent deregulation in Japan, replaced by industry self-regulation, did little to weaken trade barriers.

[15] Bernardo Bortolotti & Gianluca Fiorentini, *Barriers to Entry and the Self-Regulating Professions: Evidence from the Market for Italian Accountants*, in BERNARDO BORTOLOTTI & GIANLUCA FIORENTINI, EDS., ORGANIZED INTERESTS AND SELF-REGULATION (OXFORD, UK: OXFORD UNIVERSITY PRESS, 1999), at 131-157; and Roger Van Den Bergh, *Self-Regulation of the Medical and Legal Professions: Remaining Barriers to Competition and EC Law*, IN BERNARDO BORTOLOTTI & GIANLUCA FIORENTINI, EDS., ORGANIZED INTERESTS AND SELF-REGULATION (OXFORD, UK: OXFORD UNIVERSITY PRESS, 1999), at 89-130.

[16] In social policy regulation, critics are quick to question the extent to which firms and industries will truly restrict themselves, notwithstanding their stated intentions. To some extent, this debate rests on questions as to whether firms optimize shareholder wealth or take a stakeholder perspective. *See* Javier Núñez, *A Model of Self-Regulation*, ECONOMICS LETTERS 74, 91-97 (2001), and Maxwell, *et. al.*, Self-Regulation and Social Welfare, cited *supra* at note 11, at 52.

[17] Luigi Alberto Franzoni, *Imperfect Competition in Certification Markets*, in BERNARDO BORTOLOTTI & GIANLUCA FIORENTINI, EDS., ORGANIZED INTERESTS AND SELF-REGULATION (Oxford, UK: Oxford University Press, 1999), at 158-176.

[18] *Id.*, at 37.

The insurance industry plays a special role in certification as well, especially since certification may signal lower insurance risks, which may then be reflected in lower premiums. Not unexpectedly, insurers need to be able to rely on certifiers' independence from producers. For example, certifiers that vigorously compete for producer business may compromise the accuracy of certification (witness recent auditing scandals).[19]

Closely related to the role of insurance in certification is the role of liability. Liability, of course, already works in partnership with regulation when safety issues come into play, for neither liability nor regulation by itself is generally sufficient to produce socially desirable levels of care.[20] From a producer's perspective, then, self-regulation that results in an active compliance activity may provide protection against imputation of "intent" to undertake unlawful acts.[21] In product liability, for example, a showing of negligence usually requires all of the following elements to exist and requires all of the associated questions to be answered in the positive: (1) duty (did the vendor use "reasonable care"?), (2) breach of duty (was there unreasonable conduct involving an act or a failure to act?), (3) foreseeability (was the problem foreseeable?), (4) proximate cause (did the breach cause the damage?), and (5) damage (did the conduct cause physical injury or some other loss?). A widely accepted industry certification or a government-endorsed certification, along with a vendor's consistent effort in securing such certification, can aid a defense on questions of duty and breach of duty.

A critical question in self-regulation is the appropriate role of government. Pure self-regulation (*i.e.*, regulation without any external influence) is usually rejected based on the lack of evidence showing that this mode naturally arises or is effective.[22] Conversely, a broad correlation between evidence of governmental incentives for the creation of self-regulation and self-regulatory activity[23] seems to suggest that successful and credible self-regulation is consistently coupled with some form of influence

[19] As another example, periodic softness in the market for maritime insurance leads to lax responses to negative certification signals from insurers. *See* Frank Furger, *Accountability and Systems of Self-Governance: The Case of the Maritime Industry,* 19 LAW & POL'Y 4, 445-476 (1997).

[20] Steven Shavell, *A Model for the Optimal Use of Liability and Safety Regulation,* 15 RAND J. ECON. 2, at 271-280 (Summer 1984).

[21] *See also* John C. Ruhnka & Heidi Boerstler, *Governmental Incentives for Corporate Self-Regulation*, 17 J. BUS. ETHICS (1998), 1309-326 (1998) [hereinafter: Ruhnka & Boerstler, Governmental Incentives] (analogizing self-regulation to certain consequences that can be found in criminal antitrust cases).

[22] *Id.*, at 41-42, 45. *See also* Jorge Rivera & Peter de Leon, *Is Greener Whiter? Voluntary Environmental Performance of Western Ski Areas*, 32 THE POL'Y STUDIES J. 3. 417-437 (2004) (noting that, absent oversight, a firm that joins a self-regulatory body may actually have a tendency to underperform when compared with firms that do not join, thus effectively deriving membership benefits without actually investing in the area subject to self-regulation).

[23] *Id.*, at 51.

or oversight, leading to a model that might be described as co-regulation.[24] Such external influences may come from government entities or, as is apparent in certain contemporary social policy cases, independent non-governmental organizations with political influence or influence over consumer choice.[25] When influencing the formation of self-regulatory bodies, the government's manner of signaling its intentions can be important. In fact, game theory suggests that the government should firmly demonstrate zero tolerance of undesirable behavior and immediately invoke direct regulation if such behavior is observed.[26] On a more positive note, the government can also encourage self-regulation through a variety of positive signals regarding preferential treatment for diligent self-regulators.[27]

Three processes that are commonly present in social regulation are also potentially applicable to co-regulation. These three processes are as follows: (1) prior approval, in which firms obtain approval before engaging in an activity; (2) mandatory standards, in which firms are required to comply with the regulation and undergo monitoring; and (3) information disclosure, in which firms are required to disclose facts to buyers that they might not otherwise choose to disclose.[28] Interestingly, the framework by which self-regulation is invoked can also result in unanticipated effects. For

---

[24] *Id.*, at 54. As Sinclair points out, the tendency in some of the literature to paint command-and-control regulation and self-regulation as stark and distinct alternatives is overly restrictive: "Those who are locked into a paradigm which incorrectly assumes that choices have to be made between artificially restrictive models of self-regulation and command and control regulation are unlikely to be capable of appreciating the more nuanced opportunities for achieving both efficiency and effectiveness, which arise from complementary combination of both types of instruments." Sinclair, Self-Regulation Versus Command and Control, cited *supra* at note 13, at 532. Sinclair goes on to list the following four key components, which can be modulated to select a policy on the spectrum between command and control and self-regulation (these components are quoted verbatim) (emphasis in the original):

> the nature and extent of *regulatory compulsion*;
> the extent to which *regulatory flexibility* allows firms to accommodate their individual circumstances;
> the opportunity for *industry design input* into the negotiation and development of regulation; and
> the extent to which *win-win outcomes* are the focus of regulation.

The legal and regulatory incentives used to influence self-regulation have traditionally been (and often continue to be) primarily "punitive" in nature, though some more recent cases are shifting towards positive incentives that reward corporations for actions that encourage or assist desirable behavior. *See* Ruhnka & Boerstler, Governmental Incentives, cited *supra* at note 21.

[25] Dara O'Rourke, Outsourcing Regulation: Analyzing Nongovernmental Systems of Labor Standards and Monitoring, 31 THE POL'Y STUDIES J. 1, 1-28 (2003), and Tim Bartley, Certifying Forests and Factories: States, Social Movements, and the Rise of Private Regulation in the Apparel and Forest Products Fields, 31 POLITICS & SOCIETY 3, 433-464 (September 2003).

[26] *See* Ashby, *et. al.*, Industry Self-Regulation, cited *supra* at note 12.

[27] Ruhnka & Boerstler give as examples recognition of compliance with self-regulation as a mitigating factor for corporate regulatory violations by regulating agencies, by state and federal prosecutors, and in jury instructions and sentencing guidelines; recognition of self-reporting as a mitigating factor by prosecutors and regulators; and substitution of internal compliance for agency monitoring. Ruhnka & Boerstler, Governmental Incentives, cited *supra* at note 21.

[28] A. Ogus, *Regulatory Institutions and Structures,* 73 ANNALS OF PUBLIC AND COOPERATIVE ECONOMICS, 4, 627-648 (2002).

example, a government-crafted "voluntary agreement" may reduce industry efforts to engage in industry-devised self-regulatory activities, reducing profits and, thus, general welfare.[29] This point again suggests that government should apply credible pressure in order to motivate self-regulatory activity, while also exploiting the potential advantages of self-regulation, particularly information asymmetries between industry and government.

On a related note, another necessary element for the industrial self-regulatory component is coherent industry representation.[30] Possibilities include standards bodies, industry associations, and the consortia increasingly evident in the information and communication technology industries, although care must be taken, especially in the latter case, to mitigate the potential for exclusion and reduced competition.[31]

On a final note, software, an increasingly important product and component, differs greatly from many of the other types of products that have traditionally been certified.[32] Because software can directly affect safety, software reliability is increasingly scrutinized. Certification thus can serve the dual economic purposes of signaling quality to users and reducing the liability of producers.[33] Software often has an iterative and incremental design character, so delaying certification testing until the completion of software implementation can be quite inefficient. Consequently, certification testing is better introduced as an integral part of the internal and regression-testing stages of software design.[34] Interestingly, an organization that embeds certification testing throughout the design cycle can inculcate a culture in which the criteria used for certification become implicit organizational values (*e.g.*, by embedding security certification testing, an organization can help foster a "security culture").[35] However, implementation of broad software certification processes poses significant challenges. For instance, an organization may find it infeasible to maintain

---

[29] Thomas P. Lyon & John W. Maxwell, *Self-Regulation, Taxation, and Public Voluntary Environmental Agreements*, 87 J. PUBLIC ECON, 1453-1486 (2003).

[30] *Id.*, at 42.

[31] Richard Hawkins, *The Rise of Consortia in the Information and Communication Technology Industries: Emerging Implications for Policy*, 23 TELECOMMUNICATIONS POLICY (1999), at 159-173.

[32] It is worth noting that software has been subject to certification in a number of areas, including most notably in the area of security. The US government developed a set of security certification techniques referred to as the Orange Book.

[33] It should be noted that producers of software already have a history of limiting liability through the terms of software licenses. In light of this fact, some advocate an insurance-industry-driven certification regime akin to Underwriters Laboratory-style safety certification. Harold W. Lawson, *Infrastructure Risk Reduction*, 41 COMMUNICATIONS OF THE ACM 6, June 1998, at 120.

[34] Patricia Rodriguez-Dapena, *Software Safety Certification: A Multidomain Problem*, IEEE SOFTWARE, July-August 1999, at 31-38.

[35] Greg Goth, *Will the Cyber-UL Concept Take Hold?* IEEE SOFTWARE, July/August 2002, at 12-15.

adequate criteria to certify products that change rapidly in function and capability. In such cases, certification may be practical only if it is restricted to aspects of the system that undergo fewer changes and that can be reasonably isolated. Moreover, different types of certification give rise to different challenges. Bruce Schneier, founder of Counterpane Internet Security, Inc., a managed security company in San Jose, California, points out that certifying for security—where threats are active, intelligent, and hostile—is more challenging than certifying for safety—where threats are usually passive and random.[36]

B. Certification Examples

1. Underwriters Laboratories and Product Safety Certification

Underwriters Laboratories (UL), incorporated as a non-profit organization in 1901, was initially funded by the National Board of Fire Underwriters to prepare lists of safe products, thus demonstrating the potential benefits derived from linking certification to insurance.[37] When insurance industry funding ceased in 1916, UL became a self-sustaining organization through the collection of testing fees. Today, manufacturers are motivated to seek UL certification because (1) some customers require it, (2) many consumers recognize it as an indicator of product safety, and (3) it can reduce manufacturer liability by supporting reasonable care claims.

Safety co-regulation by government agencies and an industry certifier—Underwriters Laboratories—is apparent in two distinct models. On the one hand, the Occupational Safety and Health Administration (OSHA) sanctions Nationally Recognized Testing Laboratories through an explicit accreditation process.[38] (Whereas UL was originally the only such lab, now it is but one of several.)[39] OSHA regulations thus compel manufacturers to produce and buy certified products from accredited

---

[36] Scott Berinato, *A UL-Type Seal for Security? Don't Bet on It*, EWEEK, October 16, 2000, at 11-12.

[37] For a brief but interesting history of Underwriters Laboratories, *see* Harry Chase Brearly*, A Symbol of Safety: The Origins of Underwriters Laboratories,* in DANIEL B. KLEIN, ED., REPUTATION: STUDIES IN THE VOLUNTARY ELICITATION OF GOOD CONDUCT (ANN ARBOR, MI: THE UNIVERSITY OF MICHIGAN PRESS, 1997), at 75-84.

[38] Accreditation fees for test laboratories are on the order of $10,000. *See* U.S. Department of Labor, *Nationally Recognized Testing Laboratories; Fees; Reduction of Public Comment Period on Recognition Notices,* Federal Register Number 64:45098-45114, August 18, 1999, *available at* http://tinyurl.com/3nl4o.

[39] OSHA's decision in 1988 to create a competitive market for testing could not be the result of a strict profit motive on the part of UL, because UL is a non-profit organization. However, absent the discipline of competition, even a non-profit organization may not evolve or diligently pursue efficiency initiatives. Current UL management is undertaking a major effort to modernize and increase efficiency in the organization. *See* the *2003 UL Annual Report*, Underwriters Laboratory website, *available at* http://www.ul.com/info/UL_AR_2003.pdf. *See also* Brett Nelson, *Under Fire,* FORBES, June 21, 2004.

laboratories. The Consumer Product Safety Commission (CPSC),[40] on the other hand, has a less formal relationship with UL. The CPSC actively contributes to the content of UL standards in cases where the CPSC has a direct interest.[41] In other cases, the CPSC may use public feedback as a mechanism for influencing UL practices.[42] UL, for its part, actively invests in the government and regulator services it offers. For example, UL makes its information and consulting services available only to regulators.[43]

2. Telecommunications Certification: CableLabs and Telcordia

Historically, most U.S. social policy goals have been advanced through governmental regulation rather than through self- or co-regulation. In fact, for decades antitrust laws in the United States have provided a significant deterrent to industry development of common standards. European and other international companies, on the other hand, have a long-standing tradition of working together to form common solutions. In 1984, Congress passed the National Cooperative Research Act (NCRA) in recognition of the fact that U.S. industry can benefit through participation in collaborative standards-setting activities.[44] Accordingly, the telecommunications industry has only a very recent history of group

---

[40] *See* the U.S. Consumer Product Safety Commission website, *available at* http://www.cpsc.gov.

[41] The CPSC also participates in defining standards of other "voluntary" safety standards-setting organizations, such as ASTM International (http://www.astm.org). Further, the CPSC has the authority to directly regulate in cases where it sees sufficient safety risk by "issuing and enforcing mandatory standards or banning consumer products if no feasible standard would adequately protect the public." *Id.*

[42] Underwriters Laboratories Has Been Coming Under Fire, CONSUMERS RESEARCH, January 2000, at 40-41.

[43] *See Regulatory Authorities*, Underwriters Laboratories website, *available at* http://www.ul.com/regulators/.

[44] S. REP. NO. 98-427 (1984). The National Cooperative Research Act of 1984, Pub. L. No. 98-462, 98 Stat. 1815 (cited in 15 U.S.C. 4301), related to research and development joint ventures. In 1993, the law was rewritten to include production joint ventures in addition to research. National Cooperative Production Amendments of 1993, pub. L. No. 103-42, 107 Stat. 117 (1993):

> § 2 COOPERATIVE RESEARCH AND PRODUCTION: CONGRESSIONAL STATEMENT OF FINDINGS AND PURPOSE
>
> (a) FINDINGS - The Congress finds that -
>
> (1) technological innovation and its profitable commercialization are critical components of the ability of the United States to raise the living standards of Americans and to compete in world markets.
>
> (2) cooperative arrangements among nonaffiliated businesses in the private sector are often essential for successful technological innovation; and procompetitive cooperative innovation arrangements, and so clarification serves a useful purpose in helping to promote such arrangements; and
>
> (3) the antitrust laws have been mistakenly perceived to inhibit procompetitive cooperative innovation arrangements, and so clarification serves a useful purpose in helping to promote such arrangements.
>
> (b) Purpose - It is the purpose of this Act … to promote innovation, facilitate trade, and strengthen the competitiveness of the United States in world markets by clarifying the applicability of the rule of reason standard and establishing a procedure under which businesses may notify the Department of Justice and Federal Trade Commission of their cooperative ventures and thereby qualify for a single-damages limitation on civil antitrust liability.

15 U.S.C. 4301 (1994).

certification for equipment interoperability purposes.[45] This form of certification most directly addresses the economic motivation for certification—interoperability—which is an attribute that is both valued by buyers and difficult for them to ascertain prior to product purchase.

Cable Television Laboratories (CableLabs), a non-profit research consortium founded in 1988, was formed not long after the passage of the NCRA. Funded and controlled by cable operators (generally called multiple system operators, or MSOs) in the cable television industry, CableLabs leads the development of cable television standards, as well as provides certification and qualification testing for those standards.[46] Equipment vendors tend to ensure their designs meet CableLabs standards, and they tend to seek CableLabs certification, mainly because many MSOs require certification when making equipment purchases. MSOs, in turn, are motivated to seek out certified vendors in order to increase the supply of interoperable equipment, which makes the equipment more of a commodity (an effect observable in cable modem pricing) and promotes standardization of system design and performance. Testing is performed at CableLabs, and vendors are charged fees that range from $50,000 to $115,000 per product tested, depending on the standard to which conformance is being certified.

Telcordia Technologies, a subsidiary of Science Applications International Corporation (SAIC), is a descendant of Bell Laboratories by way of Bellcore.[47] The company has traditionally supplied standards setting, certification,[48] and other services to the Regional Bell operating companies, as well as to other telephone companies and their equipment suppliers. As is the case with the cable industry, telephony industry equipment suppliers pay for qualification testing so that they can meet the certification requirements of telephone operators. Among other areas of proficiency, Telcordia inherited unique expertise in certifying the interoperability of products with Bell company operations and management databases.

In recent years, Telcordia and the company's proprietary OSMINE (Operations Systems Modifications for the Integration of Network Elements) process have engendered sharp criticism due to the high cost of

---

[45] Tim McElligot, *Six Degrees of Preparation*, TELEPHONY, October 16, 2000, at 48-60.

[46] CableLabs standards include the Data Over Cable Services Interface Specification (DOCSIS) for cable modems and the CableHome and PacketCable specifications. *See* the CableLabs website, *available at* http://www.cablelabs.com/certqual/.

[47] Bellcore was established from parts of Bell Labs during the AT&T divestiture in 1984, and SAIC bought the organization in late 1998. Bill Pitterman, *Telcordia Technologies: The Journey to High Maturity,* 17 IEEE SOFTWARE 4, August 2000, at 89-96 [hereinafter: Pitterman, Telcordia Technologies].

[48] *See Testing Services*, the Telcordia website, *available at* http://www.telcordia.com/services/testing/ntwk_integrity.html.

testing (as much as $2M per product) and the long duration of test cycles.[49] As a result, the largest Regional Bell operating company, Verizon, created its own accreditation program, and ten labs, including Telcordia's lab, are currently accredited to certify compliance against standards important to Verizon.[50] In this case, a large firm (rather than the government) has made an investment in an attempt to create a competitive market for interoperability-oriented certification testing. Moreover, Telcordia now has to compete for certification business. Accordingly, Telcordia's business strategy has shifted away from providing sole-source research and certification (as was the case in the Bellcore era and as is similar to the case with CableLabs)[51] towards providing a broad array of services and technologies.

3. Meta-Standard Certification: ISO 9000

Nations may identify accrediting bodies that in turn accredit certification bodies.[52] Not surprisingly, the details of quality systems can vary dramatically depending on the product being manufactured or the service being provided. Meta-standard certification, then, is an attempt to provide useful certification across a very diverse and heterogeneous set of circumstances by focusing on process clarity rather than specific outcomes. One management practice meta-standard is the International Standards Organization ISO 9000 series of standards, which prescribes quality systems and their documentation and management (typically for manufacturers, although the series has been applied to service providers as well).[53] A firm seeking certification creates and documents a quality system that is both specific to its own activities and in conformance with ISO 9000 series principles. An ISO 9000 certification body (typically a commercial firm offering auditing, certification, and consulting) then audits the firm to verify system conformance with the standard and with system documentation.

---

[49] Dan O'Shea, *A Certified Mess*, TELEPHONY, January 21, 2002, at 32-39.

[50] *See* the Verizon Independent Testing Laboratories Network Equipment Building System (NEBS) Testing Certification Program (NEBS-TCP) website, *available at* http://www.verizonnebs.com/tcppage.html.

[51] The transition of Bellcore from a consortium to a supplier was partly due to increasing competition between the consortium's member Regional Bell operating companies. Such competition undermines the viability of consortia. *See* Pitterman, Telcordia Technologies, cited *supra* at note 47.

[52] In the United States, three bodies are designated as accrediting bodies: the American National Accreditation Program for Registrars of Quality Systems, the American National Standards Institute, and the Registrar Accreditation Board. *See* http://www.iso.ch/iso/en/info/ISODirectory/Country/country_US.html. National accrediting bodies may themselves be accredited by a common international organization such as the International Accreditation Forum. *See* the International Accreditation Forum website, *available at* http://www.iaf.nu/. Note that ISO itself does not accredit any organization relative to accreditation or certification.

[53] Mustafa V. Uzumeri, *ISO 9000 and Other Metastandards: Principles for Management Practice?* 11 ACADEMY OF MANAGEMENT EXECUTIVES 1, 21-36 (1997).

Companies adopt ISO 9000 for the following reasons, which appear in descending order: to meet customer certification requirements (particularly those of public sector customers), to reduce the possibility of product liability, and to increase the utility of quality improvement programs in general (consistent with the theme, broadly developed in the mid-1980s through the mid-1990s, that quality improvement increases a firm's profitability).[54] ISO 9000 certification has grown into its own industry, one that employs numerous consultants, trainers, auditors, and registrars.

As became apparent by the late 1990s, however, the correlation between ISO 9000 certification and product quality is weaker than could be hoped. Task forces in the UK evaluated this phenomenon and determined that this disparity is the result of variable quality among the broad array of certifying agencies. In other words, certification of a quality system does not necessarily take into account the possibility that commitment to the quality process may decrease post-certification or that certification may be viewed as a hurdle to cross rather than as a new quality approach that should be assimilated into the operation and culture of the organization. Recommended changes to the ISO 9000 regime include calls to (1) reduce the number of accredited registrars so that more effort can be spent on accreditation, (2) use product and quality system certifications in combination, and (3) recognize the value of just-in-time practices. Some of these changes are reflected in the more recent ISO 9001:2000 framework.[55]

4. Certification for Consumers: The Wi-Fi Alliance

The Wi-Fi Alliance is a non-profit trade association founded in 1999 and organized by equipment and component providers interested in the market for IEEE 802.11 wireless local access network equipment. The alliance had more than 200 member companies by July 2004, and it certified interoperability of more than 1,500 products between March 2000 and July 2004.[56] As with a number of other consortia, the alliance is

[54] Norman Burgess, *Lessons Learned in Quality Management – A Rational Role for Certification,* IEEE SYMPOSIUM ON PROS AND CONS OF ISO 9000 ACCREDITED CERTIFICATION 1998/421, 1/1-1/3 (March 31, 1999).

[55] *See Id*. *See also* L. Paul Dreyfus, Sanjay L. Ahire, & Maling Ebrahimpur, *The Impact of Just-in-Time Implementation and ISO 9000 Certification on Total Quality Management,* 51 IEEE TRANSACTIONS ON ENGINEERING MANAGEMENT, May 2, 2004, at 125-141, and E. Davies & M. Whyman, *ISO 9000:2000 – New ISO, New Responsibilities for Top Management,* 10 ENGINEERING MANAGEMENT JOURNAL 5, (Oct. 2000), at 244-48. *See also* Eitan Naveh & Alfred A. Marcus, *When Does the ISO 9000 Quality Assurance Standard Lead to Performance Improvement? Assimilation and Going Beyond*, 51 IEEE TRANSACTIONS ON ENGINEERING MANAGEMENT 3 (2004), at 352-63.

[56] *See* the Wi-Fi Alliance website, *available at* http://www.wi-fi.org/OpenSection/backgrounder.asp?TID=5.

intended to augment an otherwise established standards process (in this case, IEEE wireless networking) by providing interoperability certification and by building a consumer brand in order to ensure interoperability of purchased products. The Wi-Fi Alliance accredits independent testing labs as Wi-Fi Interoperability Certification Labs. These labs report results to the Wi-Fi Alliance, which in turn grants certification and the right to display appropriate Wi-Fi logos. While only Wi-Fi members can request certification, the association's wide membership suggests that barriers to membership are low; in other words, the association does not seem to substantially restrict entry in order to limit competition.

5. Self-Regulation and Voluntary Agreements in Environmental Policy

Environmental regulation has seen the most active experimentation in self-regulation of any area of social policy. A sequence of environmental disasters (Bhopal, Exxon Valdez, Three Mile Island) and a set of vocal non-governmental organizations (NGOs) combine to represent public environmental interests, but recent neo-liberal trends towards deregulation recognize both the direct and indirect costs of command-and-control regulation. The result has been a wave of self-regulatory experiments in which firms and industries enter into voluntary agreements to reduce environmental impact.[57]

The environmental self-regulation experience has been decidedly mixed and has resulted in a number of findings that are beneficial to our discussion of telecommunications emergency services self-regulation.[58] These findings include both theoretical and empirical evidence of the detrimental impact of free-riding on effective industry-wide voluntary agreements,[59] the importance of external stakeholder involvement in negotiating credible voluntary agreements,[60] the critical role of public monitoring of conformance with voluntary agreements by independent

[57] *See* T. Dietz & P. C. Stern, NEW TOOLS FOR ENVIRONMENTAL PROTECTION: EDUCATION, INFORMATION, AND VOLUNTARY MEASURES (Washington, D.C.: National Academies Press, 2002); F. Convery & F. Lévêque, *Applying Voluntary Approaches – Some Insights* in RESEARCH IN ENVIRONMENTAL VOLUNTARY APPROACHES: RESEARCH INSIGHTS FOR POLICY-MAKERS FROM THE POLICY WORKSHOP ON THE USE OF VOLUNTARY APPROACHES (Brussels, 2001).

[58] *See* T. Lookabaugh & D. C. Sicker, *Self-Regulation of E911 for VoIP: Lessons for the Cable Industry from Environmental Voluntary Agreements*, MAGNESS INSTITUTE ACADEMIC SEMINAR, San Francisco, CA, 2005.

[59] *See* A. A. King & M. J. Lenox, *Industry Self-Regulation without Sanctions: The Chemical Industry Responsible Care Program*, 43 ACADEMY OF MANAGEMENT JOURNAL 4 (2000), at 698-716; J. Rivera & P. D. Leon, *Is Greener Whiter? Voluntary Environmental Performance of Western Ski Areas* in 32 THE POLICY STUDIES JOURNAL 3 (2004), at 417-437.

[60] *See* J. Carmin, N. Darnall, *et al.*, *Stakeholder Involvement in the Design of U.S. Voluntary Environmental Programs: Does Sponsorship Matter?* in 31 POLICY STUDIES JOURNAL 4 (2003), at 527-544.

parties,[61] and the importance of a plausible threat of governmental regulation.[62]

6. Certification Evolves: Telecommunications Certification Bodies

Until the late 1990s, the regulatory procedure for standardizing and certifying devices for sale to the general public under FCC rules had not changed significantly. For example, a company that wanted to market devices that connect to the telephone network under Part 2[63] [64] or Part 68[65] of the FCC rules (described below) had to first complete a series of tests, which were either performed in the company's own laboratory or outsourced to a third party. The actual testing process tended to take anywhere from one day to one week, and the test results had to be submitted to the FCC. The centrally controlled FCC approval process took up to three months, and the device could not be properly marketed in large commercial applications until it received FCC approval. The above example highlights the FCC's device-level command-and-control approach.

The questions, then, are these: What are these FCC rules, and why is device certification relevant in this context? The answer to these questions is simple: Virtually every device that connects to the network must meet certain FCC specifications before it can appear on the market. FCC Part 2, for example, is a massive collection of technical data spanning several hundred pages. It covers international regulations, nomenclature and assignment of frequencies, and the complete table of frequency allocations. FCC Part 68, in turn, regulates the connection of terminal equipment to the telephone network, and any device that is regulated under Part 68 (*e.g.*, the limits set for intentional and unintentional radiation) must also comply with the provisions of Part 15. Part 68 is important for future wireless applications, because any change in FCC regulations or policy is likely to affect all interrelated FCC compliance regulations simultaneously. In the VoIP area, as we will see, new Internet-enabled telephones will easily span all of these areas and will require certification under many different parts of the FCC rules.

---

[61] *See* K. Harrison & W. Antweiler, *Incentives for Pollution Abatement: Regulation, Regulatory Threats, and Non-Governmental Pressures* in 22 JOURNAL OF POLICY ANALYSIS AND MANAGEMENT 3 (2003), at 361-382.

[62] *See* M. Khanna, *Non-Mandatory Approaches to Environmental Protection* in 15 JOURNAL OF ECONOMIC SURVEYS 3 (2001), at 219-324; A. Alberini & K. Segerson, *Assessing Voluntary Programs to Improve Environmental Quality* in 22 ENVIRONMENTAL AND RESOURCE ECONOMICS (2002), at 157-184.

[63] 47 CFR Ch. 1 (1998), Part 2—Frequency Allocations and Radio Treaty Matters; General Rules and Regulations.

[64] *Id.*

[65] 47 CFR Ch. 1 (1998), Part 68—Connection of Terminal Equipment to the Telephone Network.

Indeed, even the most banal wireless applications (such as cordless phones) are regulated under Part 68 (for their connection to the network), Part 15 (for their radiation limitations in a broadcasting capacity), and Part 2 (for their placement in the frequency allocation zoning map). In fact, future technologies—like VoIP devices—are likely to dramatically increase the complexity involved in adhering to FCC regulations. For example, regulators used to be able to categorize transmitters and receivers with relative ease in a bygone era when television and radio were the primary subjects of regulation. Today, however, new technological advances are supplanting these categorizations, and hybrid applications no longer fit neatly within any single FCC provision. Examples of these re-categorizations include frequencies originally intended for UHF television that have been reallocated for cellular[66] and frequencies originally intended for garage-door openers[67] that are now used for cordless phones, wireless in-home LAN, car alarms, and electronic dog fences. Categorization is quickly losing its meaning, and future regulations will likely have to address purely technical criteria rather than application-specific criteria. Although VoIP is sometimes characterized as a revolutionary technology, in terms of its development it is merely one of several hundred new devices or products entering the marketplace.

In 1998, the FCC anticipated that its rules would not be able to keep up with technological advancements, and it shifted away from its traditional command-and-control paradigm by adopting ET Docket 97-94.[68] The FCC's action amended certain rules in order to

> 1) simplify our existing equipment authorization processes; 2) deregulate the equipment authorization requirements for certain types of equipment; and 3) provide for electronic filing of applications for equipment authorization. The

[66] *See* In the Matter of an Inquiry Relative to the Future Use of the Frequency and 806-960 MHz; and Amendment of Parts 2, 18, 21, 73, 74, 89, 91 and 93 of the Rules Relative to Operations in the Land Mobile Service Between 806 and 960 MHz, 46 F.C.C.2d 752 (1974) (discussing the rulemaking procedure that deals with reallocation of UHF channels for cellular telephone services).

[67] The 2.4 GHz frequency band was originally designated for home devices, but it now includes everything from wireless networking to invisible dog fences. *See* Kenneth R. Carter, Ahmed Lahjouji, & Neal McNeil, *Unlicensed and Unshackled: A Joint OSP-OET White Paper on Unlicensed Devices and Their Regulatory Issues*, FCC Office of Engineering Technology, OSP Working Paper No. 39, May 2003, *available at* www.fcc.gov/osp/workingp.html (last visited August 15, 2003).

[68] ET Docket 97-94, Amendment of Parts 2, 15, 18 and Other Parts of the Commission's Rules to Simplify and Streamline the Equipment Authorization Process for Radio Frequency Equipment, resulting in Report and Order 13 FCC Rcd. 11415 (1998), *available at* http://www.fcc.gov/oet/dockets/et97-94/ (last visited March 11, 2005).

> proposals were designed to reduce the burden of the equipment authorization program on manufacturers.[69]

As a result, the FCC shifted the regulatory burden for approval of various devices to the private sector.[70] The thrust of this action, then, was to organize a provision for so-called Telecommunications Certification Bodies (TCBs), whose objective is to conduct various tests and certifications following essentially the same criteria previously employed by the FCC.[71] Another component of this plan was the adoption of Mutual Recognition Agreements (MRAs) to allow foreign parties to evaluate equipment conformance with U.S. technical requirements.[72] The process for approval under the new regulation is quite simple, and many expect it to have an important effect on domestic and international commerce. The case may be most significant in terms of international commerce, where European organizations have enjoyed advances in standardization through Europe-wide groups like ETSI[73] and CENELEC[74] and through country-specific groups like AFNOR (France),[75] the famous TÜV (Germany),[76] and others.[77] If a U.S. company wants to market a new device to the European Union, the company must seek out a Conformity Assessment Body (CAB) under

---

[69] FCC Report and Order, ET Docket No. 97-94 Section II (3) (April 1998), *available at* http://www.fcc.gov/Bureaus/Engineering_Technology/Orders/1998/fcc98058.txt.

[70] *See* Gen. Docket 98-16, Report No. FCC 98-338, entitled "1998 Biennial Regulatory Review – Amendment of Parts 2, 25 and 68 of the Commission's Rules to Further Streamline the Equipment Authorization Process for Radio Frequency Equipment, Modify the Equipment Authorization Process for Telephone Terminal Equipment, Implement Mutual Recognition Agreements and Begin Implementation of the Global Mobile Personal Communications by Satellite (GMPCS) Arrangements," adopted December 17, 1998, released December 23, 1998.

[71] TCBs are now captured in 47 CFR Section 2.960, and they are described on the FCC website as follows:

> The Commission may designate a Telecommunications Certification Body (TCB) to process an application to determine whether the product meets the Commission's requirements and shall issue a written grant of equipment authorization. A TCB may authorize such devices subject to Certification as the FCC except new technology devices or devices with unique RF (radio frequency) safety concerns.

FCC website, *available at* http://ftp.fcc.gov/oet/ea/procedures.html.

[72] Gen. Docket 98-16, at Section II (19). *See also* Document 98-338, Footnote 36, which points out that the FCC authorizes the delegation to MRAs, but the specific technical data must be delineated within the bilateral agreement in question: "The model APEC MRA provides that countries will identify the relevant regulations and requirements at the time they enter into bilateral agreements."

[73] *See* the European Telecommunications Standards Institute (ETSI) website, *available at* www.etsi.org. ETSI was borne out of the development of Global System for Mobile Communications (GSM) standards across Europe. *See generally* Howard A Shelanski, *Competition Policy for Mobile Broadband Networks*, 3 JOURNAL ON TELECOMM. & HIGH TECH. L. 97, 111-12 (describing GSM and its relationship with ETSI).

[74] *See* the European Committee for Electrotechnical Standardization (CENELEC) website, *available at* www.cenelec.org. *See also generally* Suzanne Laplante, *The European Union's General Product Safety Directive: Another Call for U.S. Exporters to Comply with the ISO 9000 Series*, 22 SYRACUSE J. INT'L L. & COM. 155 (1996) (describing the role of various standards-setting organizations in Europe and their relationship with certification programs like ISO 9000).

[75] *See* the Groupe AFNOR website, *available at* www.afnor.fr. *See also generally* Lori M. Wallach, *Accountable Governance in the Era of Globalization: the WTO, NAFTA and International Harmonization of Standards*, 50 U. KAN. L. REV. 823 (2002) [hereinafter: Wallach, Accountable Governance] (describing AFNOR and other state-run standards-setting organizations in Europe and elsewhere).

[76] *See* the TÜV Rheinland Group homepage, *available at* www.tuv.com.

[77] *See* Wallach, Accountable Governance, cited *supra* at note 75.

Article 10(2) of the Electromagnetic Compatibility Directive.[78] A CAB, also known in Europe simply as a "Competent Body,"[79] is similar to a TCB in the United States. The European CAB then issues a "Technical Construction File," which consists of a technical judgment regarding the overall compliance of a product. If the company receives a judgment in its favor, then the device receives the coveted "CE" mark, which can be seen on virtually all electronic devices sold worldwide.[80]

Since roughly 1998, the European process and the U.S. process have grown increasingly similar, and certification bodies (and their processes) are themselves beginning to standardize on both sides of the Atlantic. In both the European Union and the United States, companies with approved telecommunications devices are expected to keep their certification reports on file in each country where the devices are sold, and the reports must stand up to scrutiny if device approval is ever questioned. A CAB-certified (Europe) or TCB-certified (United States) device may pass all tests, but if a report does not meet with inspector approval or if incorrect test data is discovered, the company in question may be forced to suspend shipments until it presents acceptable proof of conformity. In addition to receiving certification, devices must thus be able to sustain audit.

7. An Expanded Role for Enforcement

It is within this latter inspection and "policing" capacity that the FCC will continue to perform its own independent surveillance of products on the market[81] using random product testing mechanisms and other procedures to investigate allegations of non-compliance.[82] Ultimately, however, the certification process of the delegates (the TCBs) will help to free up FCC resources, marking the beginning of an ongoing shift in the role of the FCC from command-and-control regulation to *ex post*

---

[78] The Electromagnetic Compatibility (EMC) Directive 89/336/EEC, *available at* http://tinyurl.com/4k8n4.

[79] *See* John Bengston, *Connecting Terminal Equipment Under the New EC Regs*, 9 COMPUTER LAWYER 7, 32 (1992). The article outlines the early challenges and regulations facing the European Community. The article may be somewhat outdated now, but it highlights the challenges of setting up uniformity in the pre-GSM European climate in the early 1990s.

[80] *See* the European Union's website on Electrical Equipment, *available at* http://europa.eu.int/comm/enterprise/electr_equipment/index_en.htm.

[81] For a discussion of changes made and policing functions (including fines), *see* David E. Hilliard & Kurt E. DeSoto, *FCC Refines Computer Marketing Regulations,* 9 COMPUTER LAWYER 9, 27 (1992) [hereinafter: Hilliard & DeSoto, FCC Refines Computer Marketing Regulations]. The article discusses the expansion of enforcement at the FCC level:

> [In 1992, the FCC] substantially expanded the enforcement of its computing device rules. … The penalties for marketing unauthorized or improperly tested computers or computer peripherals increased [to] (1) civil forfeitures of $75,000 for continuing violations and $10,000 each for other violations; (2) criminal penalties as high as $500,000 in fines and two years in prison; (3) civil litigation; and (4) equipment confiscation.

[82] FCC Gen. Docket No. 98-68, Report and Order, cited *infra* at note 84.

enforcement functions. Nonetheless, the FCC remains responsible for issuing certification to TCBs (a responsibility that it shares in certain cases with the National Institute of Standards and Technology),[83] and the aforementioned rules allow either the TCB or the FCC to revoke the interconnection authorization of terminal equipment.[84] Thus, the FCC still retains an important role in enforcement control, and it may even revoke equipment placed on the market after authorization has been acquired by a TCB. The law requires the FCC to prove that (1) the equipment approval has been obtained by misrepresentation, (2) the approved equipment causes harm to the public switched telephone network, (3) the responsible party willfully or repeatedly fails to comply with the terms and conditions of its equipment approval, or (4) the responsible party willfully or repeatedly fails to comply with any FCC rule, regulation, or order relating to terminal equipment under the Communications Act of 1934.

It is not yet known if the enforcement arm of the FCC will prove effective, especially in cases where a TCB certifies the commercial application of a product that subsequently interferes with other entities. Bell Atlantic raised this issue, contending that foreign certification of equipment could introduce partiality into the authorization process and lead to inconsistent application of standards. Nonetheless, anecdotal evidence suggests that the increasing number of FCC representatives at events such as COMDEX,[85] where new technologies are often shown to the public,[86] demonstrates the organization's willingness to embrace its enforcement role.

The more pressing question, however, is this: how will the FCC actually go about setting up deterrents to prevent wrongs, such as the proliferation of, say, an inexpensive, uncertified VoIP device that enters the market and takes off rapidly? It may be difficult or even impossible to recall all of the devices, especially if they realize major sales within a short

---

[83] *See* "Accreditation of Telecommunications Certification Bodies (TCBs) and Certification Bodies (CBs) under the Mutual Recognition Arrangement (MRA)," National Institute of Standards and Technology website, *available at* http://ts.nist.gov/ts/htdocs/210/gsig/tcb-program.htm (last visited March 15, 2005).

[84] *See* FCC Gen. Docket No. 98-68, Notice of Proposed Rulemaking (1998), at 15, *available at* www.fcc.gov/Bureaus/Engineering_Technology/Notices/1998/fcc98092.pdf ("[W]e anticipate that circumstances may arise where it may be necessary to suspend or revoke a TCB's certification authority"). *See also* FCC Gen Docket No. 98-68, Report and Order (1998), *available at* www.fcc.gov/Bureaus/Engineering_Technology/Orders/1998/fcc98338.pdf [hereinafter: FCC Gen. Docket 98-68, Report and Order]. A TCB may revoke a certification up to thirty days after issuance. However, after thirty days, a certification "can only be revoked by the Commission. A TCB shall notify both the applicant and the Commission when a grant is rescinded." *Id.*, at 49.

[85] COMDEX is a major technology fair that, until recently, was held annually in Las Vegas. In 2004, the organizers cancelled the event for the first time because of poor participation from vendors. *See Comdex's Organizers Cancel This Year's Show in Las Vegas*, WALL ST. JOURNAL, June 24, 2004, 2004 WLNR 7318650.

[86] *See* Hilliard & DeSoto, FCC Refines Computer Marketing Regulations, cited *supra* at note 81 (stating that in fall 1991 the FCC issued more than 100 violations to vendors who exhibited unauthorized computer equipment at COMDEX).

period of time (such as during the Christmas season). The device manufacturers could be sham organizations purchased through international e-commerce portal sites—or even offshore companies—making them very difficult to monitor from the FCC's point of view. Only through efficient delegation to third-party authorities (*e.g.,* the TCBs) will the FCC have any opportunity to allocate the resources needed to police the proliferation and e-commerce distribution of new technologies.

8. Certification Processes

Each of the preceding examples involves a certification process from which we can abstract the following common and desirable elements:

- **Pre-Certification**. Certification processes, expectations, and procedures are well-documented, and certification officials have easy access to educational and background materials. If the certification process is sufficiently complex, a third-party community of trainers, consultants, and test equipment providers will participate in certification activities. The goal is to facilitate a standard, straightforward, repeatable process. Fees are documented, predictable, and reasonable.

- **Certification**. Testing and evaluation against the certification criteria take place. Certification of easily transportable equipment occurs at specified test facilities, preferably facilities that are conveniently (or even regionally) located. Certification teams go on site to test equipment that is non-transportable and to evaluate facilities, infrastructures, or processes. Testing is prompt and transparent, and it follows designated guidelines.

- **Post-Certification**. The certifying authority follows a clear process that clarifies deadlines and formats for reporting test results. The reasons for any failures are clearly documented, and comments and recommendations are suggested. The certifying authority follows a clear and transparent procedure for questioning and appealing results and for publicizing successful certification, both by the certifier and by the certified body. A publicly accessible database contains successful certification results. The certification authority documents and institutes a periodic follow-up re-inspection process.

C. Implications for VoIP Emergency Services Certification

We can make several general observations about VoIP emergency services certification based on the preceding theories and specific examples of certification. (These observations will then inform specific recommendations provided in Section VI.) To begin, certification of emergency service capabilities for VoIP better fits the category of certification for social policy goals than certification for economic reasons, mainly because firms have not traditionally been able to charge consumers for 911 services.[87] The implication is that standards and related certification bodies are not likely to arise unless they are naturally driven by the industry's own economic interest (as is the case with TCBs such as Telcordia, CableLabs, and Wi-Fi Alliance).

General evidence suggests that social policy self-regulation requires strong external motivation. In the case of VoIP emergency services, associations of public safety officials, such as the National Emergency Number Association (NENA) and the Association of Public Safety Communications Officers, already play an active role in prompting self-regulatory discussions.[88] However, the effectiveness of this external motivation is seemingly derived largely from the presumption that these organizations have the ears of regulators at the local and federal levels. For example, no truly separate non-governmental organizations play an active regulatory role (*e.g.*, by influencing consumers). Hence, it appears likely that government influence, either direct or indirect, is needed in this case. Such influence can naturally take a number of forms. The government could inspire self-regulation through the credible threat of potential regulation, or it could actively share regulation responsibilities with social policy organizations. Moreover, although the FCC is the most obvious choice to take the reins of such social policy regulatory initiatives, government influence could also come from state agencies (assuming they can be sufficiently coordinated to be effective) or from a combination of federal and state agencies.

In short, social policy self-regulation faces a credibility challenge. Consequently, certification processes should not be held captive to the certifying body, which could make the standards subject to use in extracting

---

[87] Firms subject to rate regulation may remain relatively neutral toward the imposition of 911 requirements if they are able to recover costs through a general increase in prices. However, we expect many firms involved in VoIP to be excluded from rate regulation and consequently motivated to avoid costs without offsetting revenues unless other issues, such as the threat of government regulation, arise.

[88] *See* the National Emergency Number Association website, *available at* http://www.nena9-1-1.org/VoIP_IP/index.htm and http://www.apcointl.org.

monopoly rents (by restricting industry participation) or could induce the standards to be set at inappropriate performance levels.[89] One option here is the use of a broad-based standards-setting organization that openly invites the participation of other parties, such as government and consumer organizations. In parallel, it would be valuable to create a "hierarchy of trust" of accrediting certifiers, whereby the root accrediting organization remains credibly independent of the certified companies. This role of the root accrediting organization can be played by the government, as in the case of OSHA, or by a sufficiently independent group of institutions, as in the case of the ISO 9000 series of standards. The role should probably not be played by a major industry firm, as in the case of Verizon's testing certification lab, or by a tightly controlled industry consortium.[90]

Many certification processes that involve conformance testing are overseen by a competitive market of certifiers (*e.g.*, product safety certification, telephone company product interoperability certification, and ISO 9000 quality system certification). Such an approach may work for VoIP emergency services certification as well. Note, though, that implementation of this approach would reinforce the need for a hierarchy of accreditation so that the certifiers' capabilities can be trusted.

Furthermore, VoIP emergency services certification is likely to consist mainly of software certification. Here, it would be wise to encourage certification processes that engage with software development throughout its cycle rather than solely at the cycle's end. Also, some aspects of VoIP emergency service performance will depend on network and system characteristics that can be expected to vary widely among VoIP providers. An element of system meta-management standardization and certification, similar to ISO 9000, may be appropriate in such heterogeneous circumstances, but we need to learn from the ISO 9000 experience so that we do not rely solely on process certification to control outcomes.

In fact, consumers can play a key role in discriminating between certified and non-certified firms and between different levels of certification through their buying choices. Examples of such consumer involvement include certification by UL and the Wi-Fi Alliance. However, for the

[89] As noted earlier, standards can be set too high (in an effort to restrict competition) or too low (in an effort to reduce industry costs at the expense of overall welfare).

[90] While the Wi-Fi Alliance is clearly a membership-restricted industry consortium, it nonetheless has a fairly open membership policy; as such, it is subject to little criticism of "tight control." However, even an organization with broad industry membership risks the possibility that opaque and self-interested policies, the kind that are sufficient to undermine credibility, could be implemented.

certification to be effective, consumers need to be aware of the certification's implications and confident in its legitimacy, thus implying an investment in consumer awareness and in policing inappropriate assertions of certification. These functions can be accomplished through the combined efforts of the government and industry trade associations (*e.g.*, the Wi-Fi Alliance), both of which create a brand around certification, obtain legal rights to certification marks, and prosecute infringers, as well as by individual certified firms, which are generally motivated to promote the significance of certification in order to differentiate themselves from non-certified firms.

Finally, careful consideration of the role of insurance and liability mitigation could accelerate regulatory progress and industry participation beyond that which would be naturally motivated by the threat of government regulation. Here again, government involvement can potentially help. For example, governmental roles, such as in setting appropriate standards and serving as the root accrediting body for certifiers, can enhance the status of standards and the broad acceptance of certification. Insurance industry participation in standards setting and in institutional design of certification is also desirable if it leads to differential premiums for industry participants based on certification.

III. TECHNOLOGY ASSESSMENT

In this section, we will provide a technology assessment of VoIP emergency services based on a classification of fundamental trends in technology and protocol models. We will begin by reviewing the basic operations and functions of today's emergency services. Next, we will discuss the engineering and operations of VoIP systems. Finally, we will describe how VoIP emergency services might be implemented and offer a set of possible (preliminary) VoIP emergency services requirements.

A. Emergency Services and the PSTN

In the context of the PSTN, emergency services in the United States have long been known by the dialing convention 9-1-1.[91] When this number is dialed, an emergency call is routed to the appropriate public safety answering point (PSAP) and then routed to fire, medical, or law enforcement agencies, as appropriate. Enhanced 911 (E911) added a capability that enables the emergency services dispatcher to see the calling

[91] For background on 911, *see* "911 Services," Federal Communications Commission website*, available at* http://www.fcc.gov/911.

number and information about the caller's location. Regulations imposed on emergency services obligations vary across services, technologies, and local, national, and international borders.[92] In the United States, certain carriers are required to support 911 service (under the 911 Act),[93] with regulatory responsibility divided among federal, state, and local authorities.[94]

In traditional E911, the initial routing of a 911 call is provided by the central office, which uses a routing database to associate the caller with the appropriate PSAP. E911 provides calling number information in the Automatic Number Identification (ANI) and location information in the Automatic Location Information (ALI), and it assumes that the PSAP that receives the call is geographically related to the call origination location (this routing process is accomplished using a selective router database search). The PSAP then accesses a Public Safety-Automatic Line Information (PS-ALI) database to associate the calling number with a physical location. At this point, the PSAP may forward the call to an emergency call center, which performs another database search (on a database maintained by the telephone company) to associate the caller's phone number with a particular location.

B. Emergency Services and Wireless

Many of the problems facing VoIP emergency services are similar to those of emergency services for commercial mobile radio service ("wireless" telephony). Although the technologies are different, some of the same solution mechanisms apply. For example, the development and adoption of wireless emergency service solutions followed a long and convoluted path.[95] While many of the issues that arose were attributed to

---

[92] Although common in many respects, emergency services regulation in the European Union differs from emergency services regulation in the United States. A simple but obvious difference is the emergency number itself (911 in the United States, 112 in Europe). "Commission Recommendation on the Processing of Caller Location Information in Electronic Communication Networks for the Purpose of Location-Enhanced Emergency Call Services," July 25, 2003, *available at* http://europa.eu.int/eur-lex/pri/en/oj/dat/2003/l_189/l_18920030729en00490051.pdf).

[93] "In the Matter of Implementation of 911 Act: The Use of N11 Codes and Other Abbreviated Dialing Arrangements," Fifth Report and Order (CC Docket No. 92-105) and First Report and Order (WT Docket No. 00-110), 2001.

[94] For example, the 911 Act requires the FCC to take a leadership and support role in implanting wireless 911, but the Act does not give the FCC the authority to regulate statewide plans. "About State 911 Deployment Plans," Federal Communications Commission website*, available at* http://www.fcc.gov/911/stateplans/about.html.

[95] Dale N. Hatfield, *Challenges of Network Design in an Increasingly Deregulated, Competitive Market,* Remarks at the IEEE International Symposium, March 27, 2003, *available at* http://www.im2003.org/presentation%20files/RemarksDH_IM2003.doc. *See also A Report on the Technical and Operational Issues Impacting Wireless Enhanced 911 Services*, 2002, *available at* http://gullfoss2.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=6513296239, and Dale Hatfield, *Architecture as Policy*, in SHERRIE BOLIN, ED., THE STANDARDS EDGE: DYNAMIC TENSION (2004).

technical uncertainty (due to an inadequate level of technical understanding early in the process), a significant number of the delays were the direct result of industry resistance (due to the absence of strict timelines). Another issue to consider is whether or not certain policy approaches might hasten the development effort. In the wireless emergency services regulatory process, the FCC played a substantial role in specifying and assessing the technical characteristics of the location technology. This initiative consumed considerable time. An industry-led specification and assessment process might have hastened this process, particularly if regulatory agencies had monitored the process and set deadlines. Another issue to consider is that of the implementation process itself. Wireless emergency services made use of a phased implementation approach that considered short-term versus long-term solutions. Such an approach can help to promote interim solutions and allow for the creation of reasonable timelines for long-term solutions.[96]

One important lesson worth considering is this: past regulations should not necessarily be used to define future policy. Different technologies operate in different ways, and these variations can lead to the development of new capabilities and features. For example, as Henning Schulzrinne points out, VoIP offers a number of advantages over voice telephony, including higher resilience, faster call setup, accessibility support, multimedia support, greater cost efficiency, more call data, no telephone reliance, and greater competition.[97] In addition, unlike traditional telephony, IP phones do not need to associate with a local central office, and they have little to no need for explicit voice service providers. Instead, the functions of the provider are dispersed and require minimal provider assistance. The development of policies that do not appreciate such differences could signal the loss of technical opportunities to better serve society.

---

[96] An FCC news release describes the obligations imposed on certain carriers in terms of providing emergency services. The regulations on carriers are imposed in two phases, the first of which requires carriers to report the wireless caller's phone number at the location of the antenna that received the call. The E911 second phase requires wireless carriers to provide the precise location of a 911 caller within 50 to 100 meters. Deployment of the second phase began in October 2001 and is scheduled for completion by December 31, 2005. *See FCC Expands E911 Rules,* FCC NEWS, November 13, 2003, *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-241214A1.pdf.

[97] *See* Henning Schulzrinne, *9-1-1 Calls for Voice-Over-IP,* Ex-Parte Filing for Docket 94-102, February 28, 2003, *available at* www.cs.columbia.edu/IRT/papers/emergency.pdf.

C. VoIP Technology

In simple terms, VoIP carries speech over an IP-based network.[98] The power and complexity of VoIP come largely from its ability to separate functions that were traditionally bound together, such as transport and signaling, thereby providing many more options for each function based on ubiquitous and increasingly inexpensive IP-based networking and IP-compatible access technologies, processing, and storage.

1. VoIP Parameters

IP networks may not offer the same level of performance as circuit-switched networks for voice communications. In order to obtain a similar level of performance, we must explicitly consider specific VoIP parameters, such as encoding, delay, and transport.

On a VoIP telephone call, voice is transmitted over packet networks. This transmission requires the conversion of analog voice to a digitized form, followed by a subsequent encapsulation of the digital content into a packet technology before the content is transmitted using an access technology. The initial analog conversion process is referred to as *encoding*.[99] After the analog content has been encoded into a digital format, the information is packetized (with the help of a transport layer)[100] and passed to the access technology (*e.g.*, Ethernet) for delivery on the network. At the other end, the digital information is retrieved and converted back into

---

[98] The difference between VoIP providers and VoIP services is worth considering. VoIP as a product can be offered much like any other software application (*e.g.*, Microsoft Word). Some VoIP products can be installed on a PC and made to run with little (or no) service provider participation. Some of the simpler products include NetMeeting, which is sold by software giant Microsoft. *See* the description on Microsoft's NetMeeting website, *available at* http://www.microsoft.com/windows/netmeeting/. Vonage, a service provider, also sells a product that can be loaded onto an individual's computer. *See* the description on Vonage's website, *available at* http://www.vonage.com/features.php?feature=softphone. Such products make use of the network to reach other end points and rely on so-called "intelligence" within the product (*i.e.,* software features or information added to the product, such as through software updates). On the other hand, a VoIP service provider can augment a product by including additional functionality, routing and database capabilities, security, and more. In this model, the product may still be software, or it may be a combination of physical devices and software coupled closely to the service provider.

[99] In digital telephony over the traditional PSTN network, voice is usually encoded using PCM-u or PCM-A, resulting in a bandwidth requirement of 56-64 Kbps. However, a variety of different compression algorithms can be applied in VoIP, providing all participating terminals have the required capability. Various algorithms can introduce quality, delay, computation, and bandwidth tradeoffs. For example, G.723.1 reduces the bandwidth usage of the call to 5.3 Kbps, but it also introduces a computational delay of 67.5 ms. *See generally* DANIEL COLLINS, CARRIER GRADE VOICE OVER IP (McGraw-Hill, 2000).

[100] Typically, the Real-time Transport Protocol (RTP) adds important timing and other information relevant to voice and other time-sensitive media traffic. Next, the User Datagram Protocol (UDP) provides limited multiplexing and data detection. Unlike its peer protocol, TCP, UDP does not provide error recovery; instead, error management is left to RTP and the voice codec used. Finally, UDP packets are placed in IP packets and delivered to a specified Internet address. *See generally* COLIN PERKINS, RTP: AUDIO AND VIDEO FOR THE INTERNET (Addison-Wesley Professional Publishing, 2003).

analog form, which the listener can then understand. VoIP permits a wider range of choices and tradeoffs among performance parameters than traditional PSTN. These choices and tradeoffs include the following:

- **Distortion**. Low bit rate compression may be bandwidth efficient, but it may also distort speech.

- **Errors**. Voice traffic has some degree of error tolerance (*e.g.*, a small amount of missing information will not impact intelligibility, whereas even a small error in a financial transaction is considered intolerable). However, a high enough error rate from lost packets or errored packets degrades data intelligibility.

- **Delay**. Compression algorithms, packetization, and other stages of packet transmission induce delay. Delays in excess of 250 milliseconds can be annoying, and long delays tend to induce a half-duplex conversation in which each party pauses for a substantial period of time after speaking to determine if the other party wants to speak.

- **Loaded Networks and Quality of Service**. Both errors and delay are affected by whether or not the networks involved in transmitting the voice are loaded (*i.e.*, whether they are subject to traffic that occupies a substantial fraction of their capacity) and whether or not they have some form of prioritization capability (*i.e.*, quality of service, or QoS). Loaded networks that lack QoS typically induce long and variable delays (jitter) and sometimes drop packets.

- **Echo**. Echo, a traditional issue in analog telephony, can still be an issue in VoIP, depending on the design of the analog portions of the system.

- **Power**. Analog PSTN terminals can be powered by the phone network. Assuming that the phone network has backup power, the system (including 911 service) can remain operational even if the customer premises is without power. VoIP systems do not automatically have such a backup system (although, to be fair, neither do cordless phones, which are connected to the PSTN).

For emergency services, we are concerned with the potential impact of these characteristics on the intelligibility of calls and on users' capability to place emergency service calls during power outages.

2. VoIP Signaling

While the traditional functions of setting up and tearing down calls persist in VoIP, VoIP can augment these functions in many ways by exploiting ubiquitous IP networks and inexpensive processing and storage capabilities. VoIP signaling protocols control these functions, and these protocols continue to evolve and include several variants (in some cases competing variants, in other cases, complementary). The most important variants are the Session Initiation Protocol (SIP), H.323, media gateway protocols,[101] and a number of proprietary protocols. Here, we focus primarily on the role of SIP-based systems in supporting emergency services.

SIP,[102] a protocol developed within the Internet Engineering Task Force (IETF),[103] provides for the establishment, modification, and termination of sessions (or calls). A SIP network generally consists of user agents, proxies, registrars, and redirect servers, all interconnected via an IP network. These devices exchange messages in a process used to establish the call, and they do so in a manner analogous to the now widespread packet-signaling system used in the PSTN, Signaling System 7 (SS7). SIP could enable emergency services enhancements by providing a richer information set than ANI and ALI. For example, an individual could program a VoIP device to transmit medical records or emergency contact instructions to an emergency calling center (via SIP). Such functions, if considered highly desirable socially and executable at a reasonable cost, could easily become subjects of future social policy, or, as we suggest in this paper, self-regulation.

---

[101] Media gateway protocols include the Media Gateway Control Protocol (MGCP), MEGACO, and H.248. A media gateway might be used to interface between a VoIP network and the PSTN, and a media gateway controller interacts with the signaling systems in each domain and manages the configuration of the media gateway. The separation of voice processing from management and the capability to independently distribute the functions result in an architecture called *softswitch*. VoIP architectures in which softswitch and interfacing to the PSTN play a substantial role generally provide less end user control over system behavior. However, such constraints may aid in the implementation of traditional PSTN system functionality, including E911. In any case, this type of architecture will be important for a substantial period (likely measured in multiple decades), while VoIP and PSTN systems must coexist. *See generally* Alexandra M. Wilson, *Voice Over Internet Protocol: Ready for Prime Time,* PLI Order Number 6061, 819 PLI/Pat 421, February-March 2005 (describing the basic functionalities of VoIP and a media gateway).

[102] J. Rosenberg *et. al.*, *Session Initiation Protocol*, IETF Network Working Group Request for Comments No. 3261 (2002), *available at* http://www.ietf.org/rfc/rfc3261.txt [hereinafter, RFC 3261].

[103] Two IETF working groups, SIP and SIPPING, are active in the development of session-related protocols. These groups have developed various standards (Requests for Comments, or RFCs) and drafts, and SIP RFC 3261 represents the core protocol. *Id.*

D. Emergency Services for VoIP

As a basis for a technical model, we turn to the work of the IETF. The IETF has developed several Internet Drafts and Requests for Comments describing the potential operation of VoIP emergency services based on the use of SIP and associated protocols. In this section, we will briefly describe these works in progress and highlight areas relevant to our model. While some of these drafts will not reach maturity, we should nonetheless be able to describe a reasonable VoIP emergency services model based on this work.

We propose the following VoIP emergency services requirements, which are based loosely on work within the IETF:[104] (1) support a reasonable QoS connection,[105] (2) use a recognized emergency service number (the equivalent of 9-1-1) to identify an emergency call, (3) route calls to the appropriate response group (PSAP), (4) establish a means of locating the caller, (5) establish a means of identifying the caller, and (6) establish a means of testing the system.[106] Other concerns involving security or network operations are more general to VoIP, though they still may warrant consideration during the process of testing VoIP emergency service operations. Furthermore, mechanisms for privacy, authentication, authorization, and availability will be required.

We should note that much of the operation of SIP-based emergency services would rely on well-established and commonly deployed protocols, including SIP,[107] Domain Name Service (DNS), Realtime Transport Protocol (RTP)[108] and ENUM.[109] In addressing the functionality not provided within these specifications, we turn to various draft documents, which establish that the SIP community is resolving many of the problems associated with VoIP emergency services. A draft entitled "Emergency

---

[104] Henning Schulzrinne, *Emergency Calling*, IETF Working Document, October 18, 2004, *available at* draft-schulzrinne-sipping-emergency-arch-02. Note that IETF documents are referenced, posted, and archived in different locations on the Internet. The previous citation string should lead to the document if that string is cut and pasted it into any search engine. This citation methodology is used periodically in this section.

[105] We realize that this requirement is not a part of the IETF specifications and that many people will question its need. Nonetheless, if the communications cannot support the intended media (or negotiate a new media type), the rest of the emergency services mechanisms are moot.

[106] VoIP-based emergency services users and service providers may wish to test the operation of their service. Such testing might be motivated by reconfigurations, new installations, power outages, changes in service or service provider, changes in location, or simple maintenance testing. As the industry stands today, there really is no mechanism for consumers to complete a "test call" to E911, and the first call that consumers make is likely to be made in times of emergency. Thus, a policy and process for testing may be valuable.

[107] *See* RFC 3261, cited *supra* at note 102.

[108] RTP is the protocol used for carrying traffic such as voice and video on the Internet. *See* http://www.ietf.org/rfc/rfc1889.txt.

[109] ENUM is a domain name service that supports the translation between Internet addresses (URLs) and telephone numbers. *See generally* the ENUM website, *available at* www.enum.org.

Services for Internet Telephony Systems," for example, describes how SIP might be used to provide emergency services,[110] proposes an architecture based on existing SIP features, and makes use of DNS mechanisms to provide location mapping. A second draft entitled "Emergency Services URI for the Session Initiation Protocol"[111] defines two universal emergency SIP Uniform Resource Identifiers (URIs), which can be thought of as emergency numbers like 9-1-1, and suggests ways to increase the likelihood of being able to contact an emergency call center.

Moreover, several drafts address the problem of location identification[112] by specifying the use of object formats, privacy mechanisms, and other protocols. Other drafts propose methods of conveying user agent capabilities and profiles, both of which help to provide a fully functioning emergency system.[113] An important emergency service capability is caller authentication,[114] and the SIP specification documents authentication techniques, as do a number of draft documents. Finally, it is worth noting that the provision of VoIP emergency services needs to account for interfacing between the PSTN and VoIP networks. As indicated in greater detail below, early implementations of VoIP emergency services have been designed largely within the context of interfaced VoIP and PSTN networks, with PSAPs and emergency service responders on the PSTN side.[115]

A phased approach could be employed to replicate emergency services functionality in the SIP VoIP environment, as described by Henning

---

[110] *See* Henning Schulzrinne, SIPPING, *available at* draft-schulzrinne-sipping-emergency-arch-01.

[111] *See* Henning Schulzrinne, *Emergency Services URI for the Session Initiation Protocol*, IETF Document (work in progress), February 2004, *available at* draft-ietf-sipping-sos-00.

[112] See J. Peterson, *A Presence-based GEOPRIV Location Object Format*, IETF Document (work in progress), June 2004, *available at* draft-ietf-geopriv-pidf-lo-02. *See also* J. Polk, *Requirements for Session Initiation Protocol Location Conveyance*, IETF Document (work in progress), February 2004, *available at* draft-ietf-sipping-location-requirements-00; J. Polk, *et. al.*, *Dynamic Host Configuration Protocol Option for Coordinate-based Location Configuration Information*, IETF Document (work in progress), December 2003, *available at* draft-ietf-geopriv-dhcp-lci-option-03; Henning Schulzrinne, *Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Option for Civic Addresses*, IETF Document (work in progress), July 2004, *available at* draft-ietf-geopriv-dhcp-civil-03; and Anthony LaMarca, *et al.*, *Place Lab: Device Positioning Using Radio Beacons in the Wild, Intel Research Technical Report*, IRS-TR-04-016, October 2004, *available at* http://www.placelab.org.

[113] See D. Petrie, *A Framework for Session Initiation Protocol User Agent Profile Delivery*, IETF Document (work in progress), May 2004, *available at* draft-ietf-sipping-config-framework-03; J. Rosenberg, *Indicating User Agent Capabilities in the Session Initiation Protocol (SIP)*, IETF Document (work in progress), January 2004, *available at* draft-ietf-sip-callee-caps-03.

[114] A user authentication capability should help prevent such problems as crank calls. However, a failed authorization could result from an administrative or technical problem. Accordingly, a response mechanism and an authentication policy need to be established.

[115] *See e.g.*, http://www1.avaya.com/enterprise/whitepapers/lb1879.pdf and http://www.nena9-1-1.org/9-1-1TechStandards/Standards_PDF/NENA_03-003.pdf.

Schulzrinne and Knarig Arabshian.[116] In the simplest (and likely initial) case, the SIP elements could connect to the legacy E911 system through a PSTN gateway. In this case, the SIP device would look much like other devices commonly attached to the PSTN (*e.g.*, a private branch exchange, or PBX). This scenario requires development of little new technology, though a number of existing mechanisms would need to be considered, such as security, availability, and routing.[117] Nonetheless, a certification process could be useful in terms of ensuring the accuracy of location information.[118] Also, a labeling procedure could indicate any additional information that consumers might need. In a second case, the PSAP would be directly connected to (or "aware" of) IP network traffic. In other words, a gateway would not translate INVITE[119] messages into PSTN signaling messages; therefore, the SIP session would occur between the caller and the emergency call center. As a result, the caller and the emergency call center would be able to exchange additional information such as the patient's video or healthcare data. In this case, the routing, identification, and location information would probably still reside in telephone company databases; however, the responder could now communicate with the caller using a richer media capability (as a result of direct connectivity over IP, which is able to support multimedia communications). In a third (long-term) case, the routing, identification, and location information would now reside within the Internet, and the INVITE message would carry the traffic to the PSAP. The elements within the SIP network could gather the appropriate routing and location information using a number of mechanisms (*e.g.*, the use of DNS in mapping locations to PSAPs and emergency call centers). While the details of such a process are outside the scope of this paper, these details may nonetheless prove extremely relevant to the certification mechanisms that could be deployed.

As the preceding paragraphs suggest, VoIP emergency services could be developed by making enhancements to existing SIP-based networks. The point is that these capabilities either currently exist or will soon exist. The challenge now involves the actual implementation of these capabilities, which is where a certification process can help.

---

[116] Henning Schulzrinne & Knarig Arabshian, "Providing Emergency Services in Internet Telephony," an FCC E911 Solutions Summit, March 2004.

[117] Many security and routing technologies already exist. For example, the process of authentication and authorization could be based on existing mechanisms or SIP techniques and later could possibly be based on trait-based mechanisms currently under development.

[118] As Schulzrinne describes, location information may need to be manually configured, measured by the end system (GPS), conveyed to the end system, or provided within the network. *Id.*, at 29.

[119] An INVITE message is a used in SIP to serve as the mechanism for requesting a session (a call) with another user.

E. Technology Requirements

To assist in defining the characteristics of this process, we will next examine high-level requirements for VoIP emergency services. We propose that the certification process should first support a phased implementation. While interim solutions are available immediately, some aspects of the longer-term solution will require additional technical development, further industry negotiations (with possible regulatory intervention), and considerable investment. Therefore, as both NENA and Schulzrinne describe, a short-term solution—attaching IP devices to the PSTN emergency services in much the same way as the devices are attached to a PBX—should be available for certification now. A longer-term solution—where IP interfaces with the PSAP directly, the PSAP participates in the IP session, and the databases are IP accessible—should also be specified as soon as possible.

Together with this phased approach, we propose that the technology specifications should support a range of technologies. For example, a certification process should be developed for other IP services such as instant messaging or videophone. Further, we believe that various levels of specification should be available within a technology. For example, several levels of VoIP certification might be made available (*e.g.*, good, better, and best).

Below we propose a so-called *straw man* (a provisional, exploratory sketch) of the high-level specifications that might be required of a high-quality VoIP service (a "best" service level). Note that this service could be running as software, an IP phone, or another device.[120] Also note that we focus on certifying and labeling the VoIP end device rather than the network.

- **General capability**. provide information to end users through such means as device labeling or software notification
- **General capability**. provide reasonable quality of service (*e.g.*, meet the performance and reliability measures previously discussed)
- **System capability**. access the emergency services infrastructure
- **System capability**. form proper emergency services messages

[120] While other network requirements exist, these requirements are beyond the scope of this paper.

- **System capability**. accurately determine and communicate the proper location of VoIP applications and callers

- **End user capability**. participate in an authentication process

- **End user capability**. initiate emergency services calls using a recognized emergency number (*e.g.*, 911 or SOS)

- **End user capability**. test the emergency services applications

The details of how these requirements might be assessed remain to be determined. Furthermore, other requirements also warrant consideration (and perhaps some of the requirements listed above merit debate). Accordingly, we welcome comments and feedback.

IV. TRENDS IN CERTIFICATION AND CONSUMER PROTECTION: A BRIEF VIEW OF THE EUROPEAN AND AMERICAN APPROACHES

We have briefly seen earlier in this article that Europe and the United States have historically taken different approaches to standardization and certification and that many U.S. approaches have been borrowed from the European tradition. We have also seen that the United States and Europe are slowly harmonizing their approaches through the TCBs. How might such a collaborative concept also apply to VoIP? One way is to consider the best mechanism (European or American) for resolving the liability issues that may arise from VoIP product certification. The United States offers a consumer-action-based system of legal redress that contrasts sharply with the preventative measures taken in the European state-based social system of protections. In the United States, citizens can take legal action and seek punitive damages for relief if products do not perform as advertised or if products are defectively designed, manufactured, or labeled. In Europe, however, the state tends to take a more active role *ex ante* (*i.e.*, before products are launched into the marketplace). The European approach, then, is to rely on state-sponsored certification, to provide protections to companies that obtain such certification, and to make consumer remedies available only as a last recourse.

Europeans tend to be more precautious *ex ante* than Americans, and they tend to turn to the state (and to organizations like ETSI) to help set safety guidelines. In the case of VoIP technology, however, it is almost too late for European and American regulators to implement preventative measures of any kind. Any action, by definition, will be reactive. However, in other areas of technology—such as wireless telephony—Europeans (and to some extent Americans) have not hesitated to impose an oxymoronic *ex post* precautionary principle to an existing network of wireless telephones (the precautionary principle will be discussed in greater depth later in this section).[121] We believe that such an *ex post* approach, if applied to VoIP, will be unsuccessful, but it may prove instructive to review some of the differences between European and U.S. approaches in general. As scholar Adam Burgess explains,

> Since the 1980s, Europe has increasingly established an identity around concern about vaguely conceived threats to the health of its citizens. Unlike uncaring, free market America, in this scenario, "social" Europe is aware of the threat posed by the dangerous products of "unscrupulous" multinationals.[122]

It is perhaps helpful to understand that Adam Burgess is a sociologist who recently published a book that tracks the sociological phenomenon of the public's fear of phones (based on the "hysteria factor," discussed below).[123] In the instance cited above, Burgess purposely oversimplifies the problem—America is not "uncaring," and Europe's "aware[ness] of the threat" does not necessarily exceed that of America. What Burgess is doing, then, is making an insightful cultural point: where the United States tends to take an *ad hoc*, laissez-faire approach to consumer harms, Europe traditionally takes a more precautionary stance. These markedly different

---

[121] Fears arising from mobile phones triggered protests in Italy that called for the closure of the Vatican's broadcast facilities, led to the freezing of wireless deployment in Spain for nearly a year, and caused serious 3G deployment problems in Germany and elsewhere. As a result, many called for the *ex post* application of the precautionary principle to broadcast emissions. In Italy, the Vatican even turned down the emissions due to hysteria. *See* Yaroslov Trofimov, *Italians Say Potent Vatican Tower Emits Radiation That Poses Cancer Risk,* WALL ST. J., March 27, 2001, at B7A. Several failed U.S. cases also attempted to attach cancer liability to mobile phone manufacturers. *See Motorola v. Ward*, 478 S.E.2d. 465 (Ga. App. 1996) (rejecting a claim against a cell phone manufacturer for causing or exacerbating cancer, due to lack of causation and inconclusive evidence); *Reynard v. NEC Corp.*, 887 F. Supp. 1500 (M.D.Fla. 1995) (rejecting a plaintiff's wrongful-death action for lack of causation and for failure of the *Daubert* test); *Newman v. Motorola, Inc.*, 218 F.Supp.2d. 769 (D.Md. 2002) (rejecting a cancer claim against a cell-phone manufacturer for failure of the *Daubert* test); *Chernock v. U.S.*, 718 F.Supp. 900 (N.D.Fla. 1989) (ruling against several workers' claims against the government for injuries allegedly caused by operating radar devices); and *In re Wireless Telephone Radio Frequency Emissions Products Liability*, 248 F.Supp.2d 452 (D.Md. 2003) (preventing claims brought by five classes of phone purchasers who were not provided with headsets for use in guarding against possible danger, because federal law sets safety standards and preempts such claims).

[122] Adam Burgess, *A Precautionary Tale: The British Response to Cell Phone EMF*, 21 IEEE TECHNOLOGY AND SOCIETY 4, (2003) at 15 [hereinafter: Burgess: A Precautionary Tale].

[123] ADAM BURGESS, CELLULAR PHONES, PUBLIC FEARS, AND A CULTURE OF PRECAUTION (Cambridge University Press: 2003). Burgess seeks to explain how these fears came about in the first place—in both Europe and the United States—and uses a sociological lens to critique today's precautionary climate.

modi operandi and their impact on certification processes cannot be overlooked.

A. Different Approaches to Product Liability

Interestingly enough, the American and European approaches to liability have not always been so different, particularly since the United States once borrowed many of its laws from Europe. Indeed, every first-year American law student is familiar with a famous judgment that has had widespread implications on U.S. liability cases. In 1934, Justice Benjamin Cardozo first articulated and then dismissed the following legal principle, and he did so in the same judgment: stop, look, and reconnoiter. (Cardozo had to *first* articulate the principle and *then* dismiss it because, in the tradition of common law, the higher courts have to be clear on the precedent before reaching a different conclusion.) In plain English, this precept was originally derived from advice about stopping a car before crossing railroad tracks. However, the "reconnoiter" aspect is somewhat more complicated, for it seemingly stipulates that a driver should stop the car, get out, inspect the area and look for trains (reconnoiter), get back in the car, and, assuming no trains are approaching, cross the tracks. In this instance, Justice Cardozo noted that reconnoitering is unnecessary and quite possibly dangerous.[124] In passing this judgment, however, Cardozo reversed an earlier decision by Justice Oliver Wendell Holmes, who had decreed that an individual was obliged to get out of the vehicle and reconnoiter before crossing the tracks.[125] Not unexpectedly, Cardozo's reinterpretation of the "stop, look, and reconnoiter" provision and the greater application of that provision in the legal world have had a profound effect on the number of civil cases involving punitive damages that have been tried in the United States during the past seventy years. When Cardozo declared that individuals no longer need to reconnoiter before crossing railroad tracks, he initiated a trend that eventually placed a greater burden on railroad companies, and, in turn, on manufacturers in general. In short, the state would no longer expect individuals to take commonsense precautions to protect themselves from harm; instead, large companies would be held increasingly responsible for any damages caused by their products.

---

[124] *Pokora v. Wabash Railroad Co.*, 54 S. Ct. 580, 583-84 (1934). Justice Cardozo explained that

> [s]tandards of prudent conduct are declared at times by courts, but they are taken over from the facts of life. To get out of a vehicle and reconnoitre is an uncommon precaution, as everyday experience informs us. Besides being uncommon, it is very likely to be futile, and sometimes even dangerous. If the driver leaves his vehicle when he nears a cut or curve, he will learn nothing by getting out about the perils that lurk beyond. By the time he regains his seat and sets his car in motion, the hidden train may be upon him.

[125] *Baltimore & Ohio Ry. v. Goodman*, 275 U.S. 66 (1927).

Here, let us take a step back and look at the philosophical and linguistic underpinnings of expressions of precaution. The phrase "stop, look, and reconnoiter" is composed of an unusual mixture of English (stop, look) and French (reconnoiter, a derivative of the French word *reconnaître*).[126] Indeed, virtually all American law students have to stop, look, and reconnoiter—that is, find a dictionary—when they read the famous case, because the word *reconnoiter* is not commonly used in the English language. Indeed, the U.S. approach to consumer protection has changed drastically in recent decades, as encapsulated by the multibillion-dollar sums that tobacco plaintiffs have taken home.[127] Certainly, many of the people who have been diagnosed with or who have died from cancer as a result of smoking cigarettes did reconnoiter the damage that tobacco causes to their lungs, and yet many of these individuals and their families have sought punitive damages and have been compensated accordingly for pain, suffering, and wrongful death by the cigarette manufacturers. As it turns out, the leading U.S. cases for punitive damages have all arisen since the 1980s—and many have since been quashed by the Supreme Court.[128] So, returning to Adam Burgess' quote above, even if Burgess has oversimplified the American and European outlooks on consumer protections, he is right to say that the divergence between the two world views was set in motion at some point in the past century, possibly even in 1934 with Cardozo's ruling.

Thus, Americans arguably are no longer expected to reconnoiter; instead, large firms and multinational corporations are seemingly expected to shoulder the majority of consumer risk, and their perceived accountability for product defects and failures often translates into multimillion-dollar (or even multibillion-dollar) settlements. Nonetheless, the essence of the "stop, look, and reconnoiter" precaution lives on in both American and European culture in commonplace adages such as "an ounce of prevention is worth a pound of cure," "better safe than sorry," and "look before you leap." These expressions have Dutch,[129] French,[130] and German

---

[126] The French word *reconnaître* (and its English form, *reconnoiter*) means to *faire une reconnaissance* or, in English, to survey and review. THE COLLINS-ROBERT FRENCH DICTIONARY (1990).

[127] *See generally* Elisabeth J. Calabraser, *Unfinished Business: Reaching the Due Process Limits of Punitive Damages in Tobacco Litigation Through Unitary Classwide Adjudication*, 36 WAKE FOREST L. REV 979 (2001) (surveying and discussing the tobacco claims and the multibillion-dollar settlements and awards).

[128] *See generally* Patrick S. Ryan, *Revisiting the United States Application of Punitive Damages: Separating Myth from Reality*, 10 ILSA J. OF INT'L & COMP. L. 1, 69 (2003), *available at* http://ssrn.com/abstract=545243 [describing the development of punitive damages as a tort remedy in the United States through recent (2003) U.S. Supreme Court cases].

[129] The following common Dutch phrases are translated more-or-less directly: "beter voorkomen dan genezen" (it is better to prevent than to cure), "bezint eer ge begint" (reflect before you begin), "beter te hard geblazen dan de mond gebrand" (it is better to have blown too hard than to have burned your mouth), and "een gewaarschuwd man is er twee waard" (one warned person is worth two people).

equivalents,[131] as well as equivalents in other languages. The Hippocratic Oath, which arose out of Greece more than 2,000 years ago, has governed the actions of physicians for centuries,[132] and it offers yet another interpretation of what will become known as the "precautionary principle." According to the oath, each physician is instructed to "prescribe [a] regimen for the good of my patients according to my ability and my judgment and never do harm to anyone." Thus, while the United States has in large part replaced the "stop, look, and reconnoiter" provision with a legal mechanism for instituting punitive damages, at one point the U.S. system much more clearly resembled the European system. In tying this discussion back to the topic of VoIP telephony, however, we can see that neither Europe nor the United States has properly prepared for the new challenges that will arise from the proliferation of VoIP or for the difficulties involved in developing standards to address emergency services.

B. Technological Development Will Forge Ahead in the Face of (Pre)caution

Internet telephony will continue to develop, and the absence of an industry coalition to certify and standardize products will leave an abundance of different standards and concomitant safety problems. In fact, the market drivers for VoIP adoption are overwhelming. For example, Internet telephony will enable foreigners who live in the United States to communicate with their loved ones in their home countries at virtually no cost. Furthermore, products like KaZaA's Skype,[133] an application-layer terminal, are only in their infancy, and, regardless of what happens with the regulation of E911, these products will continue to develop and appear on the marketplace. Accordingly, the time is now to develop a certification process that affords carriers a level of protection that they can rely on.

---

[130] The most common term in French is "il vaut mieux prévenir que guérir" (it is better to prevent than to heal). Such was the title of a recent article in Switzerland asserting that the precautionary principle should be applied to "electrosmog" and to radio emissions in general. Jürg Baumann, *Smog Électrique: Mieux Vaut Prévenir que Gúerir*, 2 ENVIRONNEMENT 1999, *available at* http://www.umwelt-schweiz.ch/buwal/fr/medien/umwelt/1999_2/unterseite4/. The author says "electrosmog is omnipresent in our environment" and suggests that the precautionary principle should be applied in a proposed law that would greatly regulate and reduce the installation of new sites.

[131] The following common German phrases are translated more-or-less directly: "vorsicht ist die mutter der porzelankiste" (care is the mother of the box of chinaware), "vorbeugen ist besser als heilen" (prevention is better than cure), "man muss das uebel bei der wurzel packen" (grab evil by its roots), and "wehret den anfaengen" [resist the beginnings (of something bad)]. The latter two phrases, outgrowths of Nazi Germany, are often referred to in a political context. For a list of German aphorisms, *see* www.aphorismen.de.

[132] The Hippocratic Oath is thought to have originated some 2,300 years ago on the Greek Island of Cos. It remains today the "central document, the most often-cited summary of the physician's own understanding of what is morally required to be a good medical doctor." David L. Katz, *Perry v. Louisiana: Medical Ethics on Death Row — Is Judicial Intervention Warranted?* 4 GEORGETOWN JOURNAL OF LEGAL ETHICS 707, 714 (1991).

[133] *See* the Skype website, *available at* http://www.skype.com/.

We have already seen that inconsistent implementation of protective measures in different U.S. states seems to have inspired certain carriers to adopt subversive approaches to network deployment. For example, in spite of political maneuvers undertaken to facilitate network construction,[134] vocal community protest induced companies like Omnipoint to try to build several hundred "stealth-antenna" sites without municipal authorization during the 1990s.[135] In this particular case, Omnipoint may have concluded that the time and expense required to obtain authorization for the antennas, along with the ensuing public outcry, would have prevented it from competing successfully with existing providers who had erected antenna sites years prior. Such "stealth" deployment of wireless sites is not unlike the phenomenon that we are now experiencing with respect to new companies (like Skype) that are selling application-level software for people to run on their PCs. Before we know it, everyone's computer will be outfitted with not one but several mechanisms that enable voice communications. In the end, an industry-coordinated effort to certify these types of products may help to make the "stealth" and lesser-known solutions less attractive to consumers.

C. Government Must Respond by Encouraging Self-Regulation

More and more VoIP products are deployed each day, and we will also have to address the certification and associated liability issues that inevitably will arise. We believe that the concerted effort of various parties (*e.g.,* academics, consumers, governments, and non-governmental organizations) will be required to ensure that the growth and deployment of VoIP occur in a sensible way that protects consumers by allowing them access to emergency services. Moreover, even though the effort will need to be coordinated by these various stakeholders, industry must leap to the

[134] *See* House Report 104-204 at 95 (1995), reprinted in 1996 U.S.C.A.N.N. 10, 61-62. The report reveals Congress's intent to achieve national uniformity over radio frequency emissions standards and notes the interplay between these standards and local zoning laws:

> The [Commerce] Committee has received substantial evidence that local zoning decisions, while responsive to local concern about the potential effects of radio frequency emission levels, are at times not supported by scientific and medical evidence. A high quality national wireless telecommunications network cannot exist if each of its component [sic] must meet different RF [radio frequency] standards in each community. The Committee believes the [FCC] rulemaking on this issue (ET Docket 93-62) should contain adequate, appropriate and necessary levels of protection to the public, and needs to be completed expeditiously.

[135] *See* John Cichowski, *Antenna Critics Demand Answers*, THE RECORD [Bergen County, NJ], September 4, 1997, at L3. Cichowski discusses Omnipoint's arrangement with the State of New Jersey to put up 122 sites without municipal approval. Because of political pressure, the New Jersey Governor stepped in to provide the municipalities with a veto right. The article also discusses Omnipoint's "stealth" erection of these sites in a commercial zone without first obtaining zoning approval. Leslie Haggin, *Complaints Force Down Cell Phone Antenna,* THE RECORD [Bergen County, NJ], May 9, 1997. Haggin discusses an Omnipoint cellular phone antenna that was erected on the side of the Newark Pompton Turnpike without any zoning approval. Municipal authorities forced the antenna to be taken down.

forefront of this initiative. Along these lines, the government will have to abandon its attempts to control development—particularly in cases where development cannot be controlled—and encourage industry to collaborate in a self-regulatory effort.

As we have already seen, the government has relaxed antitrust regulation to allow industry consortia to conduct joint research and development (through the NCRA). This trend must continue. In the words of science writer Robert Pool,

> [f]or better or worse, technology has changed. Our days of innocence, when machines were solely a product of larger-than-life inventors and hardworking engineers, are gone. Increasingly, technology will be a joint effort, with its design shaped not only by engineers and executives but also psychologists, political scientists, management theorists, risk specialists, regulators and courts, and the general public. It will not be a neat system. It is probably not the best system. But, given the power and complexity of modern technology, it is likely our only choice.[136]

Pool encourages us to embrace the future development of technologies and to increase our awareness of the roles and impact of these technologies. As he notes, the "power and complexity of modern technology" warrant implementation of a proactive, multidisciplinary, cooperative approach that addresses the challenges of our increasingly technological world.

Of course, the idea that Robert Pool's "joint [product development] effort" is really our "only choice" might be challenged by some skeptics. However, the concept is a useful construct for the fast-changing technology sector, particularly in areas—like VoIP—where government regulation has proven that it has difficulty in keeping up with progress.

D. An Ounce of Precaution Is Better Than a Pound of Precaution, Particularly When the Opportunity Is Lost

We have previously seen that the development of emergency services and wireless technologies can be analogized to the development of VoIP. Europeans, for example, have attempted to apply the precautionary principle in wireless deployments. Accordingly, for our purposes it might

---

[136] ROBERT POOL, BEYOND ENGINEERING: HOW SOCIETY SHAPES TECHNOLOGY (Oxford University Press, 1997), at 305.

be useful to briefly explore the possible application of this principle in E911 and VoIP deployments and then dismiss that same possibility (much like Justice Cardozo did when he ruled that individuals may need to stop and look but that they do not need to reconnoiter).

The precautionary principle is a powerful—but extreme—example of governments' constant struggle between encouraging the development of new and exciting technologies and exerting control over those technologies so as to protect the citizenry. In attempting to define the precautionary principle and bring form to its manifold vague shapes, many scholars have traced the roots of the principle to German law—the *Vorsorgeprinzip*[137]—particularly in connection with environmental policy.[138] The *Vorsorgeprinzip* origins of the precautionary principle are based on the rationale that, as Konrad von Moltke notes, "[e]nvironmental policy is not fully accomplished by warding off imminent hazards and the elimination of damage which has occurred. Precautionary environmental policy requires furthermore that natural resources are protected and demands on them are made with care."[139] The precautionary principle finds its natural home in environmental law,[140] but its exact meaning and the manner in which it should be applied elsewhere—such as to various aspects of telephony regulation—are subjects of great debate and controversy.[141]

---

[137] *Vorsorgeprinzip,* translated literally, means "foresight principle" or "forecaring principle." A typically vague clarification of what the precautionary principle means can be found in an article written by Nicola Notaro, *Environmental Policy*, in GABRIEL GLÖCKNER, ET. AL, GUIDE TO EU POLICIES (Bruges: 1998), at 229 [hereinafter: Notaro, Environmental Policy]. The author notes that the precautionary principle is part of European law and draws a connection between the principle and the *Vorsorgeprinzip*, though he stops short of any meaningful discussion of its meaning. His entire discussion of the precautionary principle is as follows:

> [The] precautionary principle was added to the [Treaty of the European Union] and stems from German environmental law where it is known as the Vorsorgeprinzip. The principle is that whenever there is a strong suspicion that a certain activity may have environmentally harmful consequences, it is better to act before the damage occurs rather than wait for incontrovertible scientific evidence.

[138] *See* Katherine Barrett & Joel Tickner, *Trans-Atlantic Consumer Dialogue Briefing Paper on the Precautionary Principle*, Working Paper of the University of Massachusetts Lowell Center for Sustainable Production, April 23, 2001. The authors discuss the origins of the Vorsorgeprinzip, associating it with the modern precautionary principle, and attribute its origins to a West German movement during the early 1970s. The authors emphasize, however, that the meaning of the term has changed since the 1970s: "It is critical to note that the Germans viewed Vorsorge as a means of stimulating innovation and social planning for sustainability, rather than simply a tool to block potentially dangerous activities." *Id.*, at 1.

[139] Konrad von Moltke, *The Vorsorgeprinzip in West German Environmental Policy*, in TWELFTH REPORT: BEST PRACTICAL CONTROL OPTIONS (Royal Commission on Environmental Pollution, 1988), at 3.

[140] *See* Notaro, Environmental Policy, cited *supra* at note 137 (discussing the precautionary principle in the context of European environmental policy).

[141] *See e.g.*, Cass Sunstein, *Beyond the Precautionary Principle*, 151 U. PA. L REV. 1003 (2003) [hereinafter: Sunstein, Precautionary Principle]. Professor Sunstein is a heavy critic of the principle. Sunstein "challenge[s] the precautionary principle here, not because it leads in bad directions, but because, read for all that it is worth, it leads in no direction at all. The principle threatens to be paralyzing, forbidding regulation, inaction, and every step in between."

Scholars have invested great time and energy in investigating the origins of the precautionary principle and its application to science.[142] While it is correct to credit Germany with the principle's metamorphosis into a legal norm, it is perhaps more useful to recognize the principle's more general derivation. Simply put, the precautionary principle is—at best—just a *principle*. Thus, the principle is *not* law, even if it is mentioned in the Treaty for the European Union and other international laws in the United States, Germany, and elsewhere.[143] Kenneth Foster, for one, has examined the precautionary principle as it specifically applies (or could apply) to mobile phones. Foster, an international expert on the effects of wireless signals on human safety, has reached the following conclusions:

> The Precautionary Principle is not a scientific proposition, nor is it a precisely defined proposition in international law; there is some question whether it even qualifies as being a "principle" at all. Rather, *it is a counsel for risk aversion*, expressed in varying ways in numerous treaties and other documents. In practice, its application is constrained by policies, statutes and case law of individual states and international law.[144]

Indeed, as Foster has suggested, the precautionary principle is no more than "counsel for risk aversion," the kind that can be found both in our legal systems and in everyday aphorisms (*e.g.,* "better safe than sorry"). So, while it may be helpful for lawyers to take note of the German movement that incorporated the *Vorsorgeprinzip* into environmental law in the 1970s and 1980s, it is somewhat shortsighted to draw wide-ranging conclusions from the German movement.

Thus, though we have gained a greater understanding of the origins of the precautionary principle, we are nonetheless left with the following questions: Should precautions, or, more specifically, the precautionary principle, be applied to mobile phone safety? To Internet telephony? The answer to these questions—deceptively—is both *yes* and *no*. As might be expected, the general confusion as to how to apply the principle only

[142] *Id*. (noting the German origins of the precautionary principle).

[143] *See e.g.*, the Montreal Protocol on Substances That Deplete the Ozone Layer, September 16, 1987, 26 I.L.M. 1550, 1551 (applying the precautionary principle by treaty to the ozone layer); UNECD Text on Protection of Oceans, U.N. GAOR, 4th Sessions, UN Coc. A/CONF.151/PC/100/Add.21 (1991) (applying the precautionary principle by international treaty to the coast); and the Cartagena Protocol on Biosafety to the Convention on Biological Diversity, January 29, 2000, 29 I.L.M. 1027, 1031 (2000) (applying the precautionary principle generally to living organisms).

[144] Kenneth R. Foster, "Can Electromagnetic Fields Trigger the Precautionary Principle?" Presentation at the WHO/NIEHS/EC Conference on the Precautionary Principle, Luxembourg, February 2003, at 2 (emphasis added).

increases when it is applied within the context of telephony and the different technologies associated with it.[145] Naturally, we should be cautious, even *pre*cautious, about products on the marketplace. However, the precautionary principle should not be applied as a matter of law, if for no other reason than the fact that it is *not* law. Accordingly, as we turn to our proposed model for regulation, we wish to emphasize that the unfortunate alternative to a self-regulatory certification process may be the largely unproductive *ex post* application of precaution through some form of the precautionary principle.

V. A PROPOSED MODEL

In this section, we will present a specific institutional framework and a set of summary technical criteria and procedure recommendations in order to provide a concrete model of a capability for emergency services self-regulation and certification. We recognize that other models could be developed. However, this proposed model represents our best recommendation based on our current information and understanding.

A. Institutional Design

Here we refine the general observations of Section III into the following recommendation:

> Government agencies should perform some initial coordination between federal and state levels and then publicize a consistent and credible statement of intent to regulate VoIP emergency services unless credible self-regulation emerges. At the same time, government agencies should move to facilitate successful self-regulation, as described below.

1. Industry Should Organize

Industry service and equipment providers should form an organization to pursue VoIP emergency services. Such an organization could be a derivative of an existing industry trade association or consortium, and it should have the following characteristics: (1) It should be funded by and heavily involve industry participants, (2) it should remain intentionally open and transparent to all industry participants and other stakeholders, particularly regulators and consumer interest groups (such arrangements should be codified in the organization's bylaws), and (3) it

[145] *See* Burgess, A Precautionary Tale, cited *supra* at note 122, at 15.

should develop standards, as well as update and extend them. Traditional open standards bodies such as IETF, the ISO, and the American National Standards Institute (ANSI) can serve as models. Although the body would initially focus on emergency services, it could eventually embrace other social policy self-regulation goals as well.[146] This organization should also do the following: create a brand around the certification, establish the appropriate legal protections, act as a co-sponsor with the government to promote public awareness of the certification, maintain a database of accreditations, and police accreditations. The standardization activity would draw on the momentum built by the Voice on the Net (VON) Coalition, an alliance between NENA and several VoIP industry participants. The VON Coalition is described in more detail on the following pages.

2. A Separation of Powers Should Be Established

While organizing industry into consortia for appropriate standards-setting efforts is a great start, we believe an additional step is needed. In particular, the process should not be held captive to the interests of certified parties. Concretely, we recommend implementation of two specific "separation of power" elements in order to enhance the credibility of the process. First, multiple independent and competitive testing organizations should perform accreditation. Furthermore, either these organizations or third parties should provide pre-certification consulting and training. Second, these testing organizations should be accredited by a third party, distinct from both the standards-setting and certification branding organization and from the testing organizations. The two major candidates for this role are a government agency and an independent institution (*e.g.*, a respected neutral institution such as ANSI).

3. Industry and Government Should Work Hand in Hand

In order to facilitate these ends, government agencies should appoint personnel to assist in the formation of the self-regulation process as follows:

- Credibly transmit the threat of government regulation if self-regulation fails.

[146] We would not expect the motivation for new social policy goals to arise naturally from the industry participants in this organization. As we have indicated elsewhere, an external motivation is needed. Most likely, such a motivation would come in the form of a public debate culminating in a credible threat of government intervention. The close coordination with government that we are proposing could facilitate the efficient signaling of such events.

- Report back to the government the level of progress made.

- Ensure agency experts provide input into certification standards and process design.

- Promote self-regulation elsewhere in government by recognizing self-regulatory efforts as mitigating factors in punitive proceedings.

- Educate users about certification (both industry and government should cosponsor this goal).

- Work with the telecommunications industry in order to incorporate the insurance industry in the process and clarify the level of liability mitigation (beyond government liability mitigation) provided to those who diligently certify products.

- Liaise with other interested government parties (*e.g.*, Congress).

Although the preceding responsibilities will require significant effort, their implementation will require dramatically less effort than that required to create and execute government command-and-control regulation. That said, it should be clear that we are by no means advocating a passive government role.

B. Technical Approach

Ideally, this transition to an IP-based emergency services solution should not burden future models with legacy assumptions. The design, function, and operation of the Internet provide an abundant set of possible solutions, and policy addressing future emergency services should embrace this flexibility and optimize the potential social benefits. The policy thus (1) should not restrict the manner in which a function is provided, (2) should support multiple implementation methods, (3) should encourage the incorporation of emergency services into other technologies, and (4) should encourage developers to create cheaper, better, and more feature-rich technologies.

Certification will likely need to include both certification of *terminals* (which can potentially be transported to a test site) and certification of *network characteristics* (which cannot). In this paper, we focus only on the former, mainly because it is difficult, if not impossible, to exhaustively test all network nodes and usage combinations as a part of certification. With these thoughts in mind, we suggest that network testing use a meta-standard style process certification focused on (1) the way in which the network is designed and managed to maintain an emergency services capability and (2) random performance testing of particular nodes and situations.

We expect that the diversity of possible VoIP systems will preclude the possibility of certification to a single level of performance. We also believe that this diversity should be encouraged. Consequently, we propose that different levels of capability be certified, keeping in mind that the number of levels needs to be small enough that consumers can distinguish them. VoIP systems might, for example, have two certification levels: a carrier grade level (with significant requirements) and a non-carrier grade level (with less strenuous requirements).

As part of our proposed implementation plan, we recommend the use of the stages suggested in the NENA/VON Coalition initial agreement on VoIP emergency services.[147] These stages, or phases, are as follows:

- Phase One Certification (based on the NENA/VON Coalition "interim solution")
  —Deliver a 911 call through the existing 911 network
  —Provide a callback number to PSAP
  —Provide initial location information to PSAP (optional)

- Phase Two Certification (based on the NENA/VON Coalition "long-term solution")
  —Deliver a 911 call through an IP network to an IP-connected PSAP (or through an existing 911 network if PSAP is not IP-connected)
  —Provide a callback number/recontact information to PSAP
  —Provide caller location information to PSAP

This phased approach enables near-immediate implementation of emergency services. It also encourages a move away from traditional emergency services toward a more competitive environment.

[147] The VON Coalition Initial Agreement, December 2003, *available at* http://www.nena9-1-1.org/VoIP_IP/VOIP-NENA%20Actual%20Agreement.pdf. Note that this agreement was reached by the following industry participants: 8x8, AT&T Consumer Services, BroadSoft, Dialpad, ITXC, Level 3 Communications LLC, Level 3 Enhanced Services, PointOne, pulver.com, VON Coalition, Vonage, and Webley.

C. Labeling

Throughout this paper, we have noted that labeling could be an important aspect of the certification process. While the details of such a mechanism warrant a separate analysis, here we briefly propose a labeling initiative, discuss its merits, and provide suggestions regarding the manner in which it might be used.

We envision that labeling might include such concrete (and diverse) elements as (1) an identifiable sticker attached to IP phones showing the name of the certifying organization and the address of a website that provides certification details and updates, (2) a software window that periodically reminds users of emergency services specifications (possibly when the device or software detects some configuration change), and/or (3) an email sent to the user when the network detects a change in its configuration.

By tying the operation of the label to system changes, the label becomes a dynamic mechanism that could become very useful in situations when the network and the device cannot automate the proper operation of the emergency services system (*i.e.*, when a user might need to intervene). Lastly, considering the litigious nature of our society, labeling likely provides some legal protection to the VoIP service or software provider.

In sum, labeling could be used to provide users with information about the (1) availability or lack of emergency services support, (2) emergency services limitations, (3) configuration requirements, (4) configuration changes, and (5) alternative methods of summoning help.

VI. CONCLUSION

While the telecommunications industry has proven adept at self-regulating in areas of interoperability, social policy regulation has historically been the purview of the government. The diversity engendered through the transition to VoIP will challenge such command-and-control regulatory policies, and we believe the time has come to consider the alternative of social policy self-regulation. We recognize the key challenges that arise from a self-regulatory process, but we believe that the framework we have recommended can succeed. Success in this area would not only provide substantial value in the case of VoIP emergency services, but it would also add a vital new regulatory approach for use within the telecommunications industry, which continues to evolve rapidly.

VoIP technology enables a much broader range of technical and business approaches than were feasible in the PSTN world. On the one hand, this new technical reality heralds a new era of innovation and flexibility for users, while on the other hand it makes difficult (or, more likely, impossible) the task of mapping traditional social policy goals and constructs from the PSTN world to the VoIP world in a straightforward manner. We will want to preserve many current social policy goals in one form or another, as well as consider new policy goals over time. With these thoughts in mind, it seems we would be well-served by a more flexible, rapid, and innovative method of mapping such goals onto the increasingly heterogeneous world of telecommunications.

Emergency services are a critically important and immediate case in point. Traditional emergency services expectations include connection of timely, highly intelligible emergency calls with the appropriate answering point and communication of critical information regarding the call's place of origin (both as a network address and as a physical location). The variety of VoIP implementations makes these expectations intrinsically difficult to meet. Thus, we propose that industry should design—using input from the government and other stakeholders—a multi-tier certification scheme that will provide a VoIP emergency services capability that can fully satisfy these expectations. We expect the certification regime to focus on several key technical characteristics of VoIP systems, including addressing, routing, location, security, availability, and related network and application standards.

Our analysis is not complete in some important respects. From the technology perspective, we would like to further develop a broad set of technology categories that might be based on media type, network access, user expectations, or some other criteria. Within these categories, we would define a set of characteristics upon which a certification process could be applied (as we have done above for VoIP). While we have performed some basic legal analysis and inquiry into the role of standardization and consortia in institutional design, we believe that more research is needed in this area. We have not considered, for example, how social policy funding will be affected by the transition to VoIP (*e.g.*, telecommunications industry taxation helps to fund public safety, and it will be important to determine if these obligations will be transferred to VoIP or if they will be covered in some other way). Finally, we briefly discussed the importance of developing different categories of VoIP implementations against which different certification standards might be developed. We believe further investigation could allow this approach to expand to include other types of media over IP (*e.g.*, instant messages and video).

Finally, our proposed model needs both refinement and assessment. For our part, we have evaluated the model by performing critical and documented analysis of internal integrity and credibility with respect to successful precedents and by disseminating this analysis to policy-oriented audiences for critique and debate (as we have done with our submission of a preliminary version of this paper to the Telecommunications Policy Research Conference.)[148] Moreover, we have used the analysis from sections II and III to demonstrate the validity of our approach. For the longer term, we derived this analysis through the use of our particular model, as well as through our execution of specific strategies for assessing that model once it is implemented. As part of our strategy, we (1) monitored elements that evolved beyond the scope of our technical and business model, (2) tracked specific performance metrics of certified processes and compared that data against criteria derived from consumer expectations and social policy goals, and (3) compared voluntary adoption rates of certification against a template derived from our experience in industry-sponsored certification processes. This longer-term assessment represents an ongoing effort that can benefit greatly from reader feedback. To that end, we welcome comments.

[148] *See* www.tprc.org.