A dynamic assessment of VoIP adoption, innovation and their interaction with CALEA regulation

Chintan Vaishnav
chintanv@mit.edu
Engineering Systems Division
Massachusetts Institute of Technology

Charles Fine
charley@mit.edu
Engineering Systems Division and Sloan School of Management
Massachusetts Institute of Technology

Introduction

The need to expand Communications Assistance for the Law Enforcement Act (CALEA), also known as the wiretapping act, to VoIP is situated in a socio-technical context that is starkly different from the first passing of the act in 1994. A socio-technical context that is marked by service delivery models where the access provider and the service provider are separate entities, technology such as packet-switching that is not conducive to wiretapping, political environment where the law enforcement agencies (LEAs) are paranoid about homeland security and, the Internet-criminal who is savvy about their choice of encryption and other VoIP innovations. Such a system can be envisioned as a complex feedback system where, regulatory decisions lead to technology and investment choices by the industry and the consumer which may have repercussions on the adequacy of the very decision that led to these choices. In such a system, are there ways to model the cause and effect of regulatory decisions that may be dispersed in time and space?

In this paper we present a system dynamics model to understand the complex feedback system surrounding VoIP adoption, innovation and the current VoIP CALEA proceedings. System dynamics is a methodology for studying and managing complex feedback systems using a computer simulation. We model the adoption of the "managed" (facility-based or VoIP that interconnects with PSTN) and "unmanaged" (peer-to-peer) VoIP to understand the fraction of VoIP that will be under the CALEA jurisdiction. We then model the cost of compliance for the providers of the managed VoIP service and the resulting incentive structure for the new entrants to provide the unmanaged service, instead. Finally, we model the trends of the number of lawful intercepts required annually and the fraction of network that will have the CALEA-compliant technology deployed to carryout such enforcement wiretaps. Our model provides a framework as well as a computer simulation for understanding the overall CALEA compliance in a network, the cost of compliance as affected by various factors.

Several policy lessons emerge through the process of model building, falsification, calibration and the subsequent sensitivity analysis. First, the current decision of exempting the unmanaged VoIP from CALEA obligations creates an incentive

structure for its increased adoption. Second, if unmanaged VoIP aspires to be a telephony substitute, it will invite the threat of social regulation. Third, arms race between CALEA-compliant and non-compliant technologies can substantially raise the cost of CALEA compliance. Fourth, the LEA may choose to ban the use of certain encryption techniques to increase the ability to wiretap criminals; however, this would simultaneously reduce the consumer privacy protection and thereby the adoption of technology.

The rest of the paper is organized as follows. We first discuss the CALEA obligations from the old act. Next, we discuss a classification of the current VoIP business models as appropriate for our analysis. Then, we discuss the recent regulatory intervention to CALEA for VoIP and the incentive structure it creates for the various stakeholders involved. After briefly discussing the model parameterization and validation, we will end the discussion with policy analysis and lessons.

CALEA: The old act and the regulatory obligations

The Communications Assistance for the Law Enforcement Act (CALEA) requires a "telecommunications carrier" to engineer their networks to be able to:

1. Provide content tracing (lawful intercept) capability,
2. Provide call-identifying information,
3. Ensure security of the tapped communication, and
4. Ensure privacy of the user

In this section, we will provide the statutory history behind the emergence of these obligations. Our approach here is to provide minimal citation to clarify the intent of the act. For a reader with little or no legal background, we have attempted to paraphrase the act without taking too much liberty.

> In the *Second Report and Order* ("*Second R&O*"), the FCC concluded that the term "telecommunications carrier" can be applied to particular carriers, their offerings and facilities.[1] The *Second R&O* further stated that CALEA does not apply to certain entities and services, *e.g.* information services and private network services. Additionally, the *Second R&O* stated that CALEA's definitions of "telecommunications carrier" and "information services" were subsequently not modified by the Telecommunications Act of 1996.
>
> Section 103 of CALEA establishes four general "assistance capability requirements" that telecommunications carriers must meet to achieve compliance with CALEA.[2] A telecommunications carrier shall ensure that its equipment, facilities, or services that provide a

[1]Communications Assistance for Law Enforcement Act, CC Docket No. 97-213, Second Report and Order, 15 FCC Rcd 7105 (2000), at 7110, ¶ 9. The Second R&O stated that the legislative history contains examples of the types of service providers subject to CALEA: "The definition of 'telecommunications carrier' includes such service providers as local exchange carriers, interexchange carriers, competitive access providers, cellular carriers, providers of personal communications services, satellite-based service providers, cable operators, and electric and other utilities that provide telecommunications services for hire to the public, and any other wireline or wireless service for hire to the public." Id. at 7111, ¶ 10, citing 140 Cong. Rec. H-10779 (daily ed. October 7, 1994) (statement of Rep. Hyde). See also H.R. Rep. No. 103-827(I), at 23, reprinted in 1994 U.S.C.C.A.N. 3489, 3500.

[2]Section 103(a)(1)-(4) of CALEA, 47 U.S.C. § 1002(a)(1)-(4).

customer or subscriber with the ability to originate, terminate, or direct communications are capable of:

(1) expeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, to intercept, to the exclusion of any other communications, all wire and electronic communications carried by the carrier within a service area to or from equipment, facilities, or services of a subscriber of such carrier concurrently with their transmission to or from the subscriber's equipment, facility, or service, or at such later time as may be acceptable to the government;

(2) expeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, to access call-identifying information that is reasonably available[3] to the carrier (a) before, during, or immediately after the transmission of a wire or electronic communication (or at such later time as may be acceptable to the government) and (b) in a manner that allows it to be associated with the communication to which it pertains;

(3) delivering intercepted communications and call-identifying information to the government, pursuant to a court order or other lawful authorization, in a format such that they may be transmitted by means of equipment, facilities, or services procured by the government to a location other than the premises of the carrier; and

(4) facilitating authorized communications interceptions and access to call-identifying information unobtrusively and with a minimum of interference with any subscriber's telecommunications service and in a manner that protects (a) the privacy and security of communications and call-identifying information not authorized to be intercepted and (b) information regarding the government's interception of communications and access to call-identifying information.[4]

Section 104 of CALEA sets forth notices of maximum and actual capacity requirements to accommodate all electronic surveillance events that telecommunications carriers may need to conduct for LEAs.

Section 109 of CALEA addresses the payment of costs by the Attorney General to telecommunications carriers who comply with the capability requirements of section 103. The statute distinguishes between equipment, facilities and services installed or deployed on or before January 1, 1995, and after that date.

Business Models for delivering VoIP

Let us now look at the various business models and their characteristics important for meeting the above CALEA obligations. Since the introduction of VocalTec's VocalChat PC-to-PC communication software in March of 1995, VoIP-based service has steadily grown to be a serious competitor to Public Switched Telephone Network (PSTN). Various business models have emerged over time for offering VoIP as a service.

The earliest effort for large scale commercialization was by equipment-makers in 1997-1998 with their thrust to develop IP-Gateways that could convert an incoming circuit-switched call to packet-switched and vice versa. IP Gateways allowed long-distance

---

[3]CALEA does not define or interpret the term "reasonably available."

[4]47 U.S.C. § 1002(a)(1)-(4). "Call-identifying information" is defined in section 102(2) of CALEA as "dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber by means of any equipment, facility, or service of a telecommunications carrier." 47 U.S.C. § 1001(2). For a discussion of call-identifying information, *see*, *supra*.

companies such as AT&T, MCI to convert their circuit-switched backbone to *VoIP in the backbone*. While many argue that this approach leads to a better use of bandwidth, it is clear that the statistical aggregation in the PSTN was nearly perfect, so the efficiency gain from IP backbone couldn't have been that much. VoIP in the backbone, however, did offer the long-distance companies a way to avoid access charges between their high-traffic nodes.

Since the year 2000, three other business models for VoIP-based service have emerged. Local or long-distance companies such as QWest owning DSL facilities, or cable companies such as Comcast owning cable facilities have begun to offer *Facility-based VoIP*. Proliferation of broadband has now made possible for companies such as Vonage to offer VoIP service over an existing broadband connection (*VoIP over Broadband*) or companies such as Skype, Yahoo and AOL to offer a free application for peer-to-peer (P2P) voice communication (*P2P VoIP)*. Table 1 shows the four business models. Of course, the above is one of many ways of categorizing VoIP business models. We have chosen this classification as it provides a reasonably clear categorization for thinking about the regulatory issues. The business models differ on many accounts, but let us focus on only those differences that matter for CALEA.

Business Models	***VoIP in the Backbone***	***Facility-based VoIP***	***VoIP over Broadband***	***P2P VoIP***
Examples	AT&T, MCI, Sprint	Qwest DSL, Comcast	Vonage, 8x8, SkypeOut/ SkypeIn	Skype, Yahoo Messenger, IM
PSTN Inter-connection?	Yes	Yes	Yes	No
Ownership	Same operator and service provider	Same operator and service provider	Different operator and service provider	Different operator and service provider
Technology to connect the end device	Circuit Switching	Packet Switching	Packet Switching	Packet Switching

Table 1 VoIP business models and their differences pertinent to CALEA

First, is the interconnection with PSTN. Business models that allow for calling a PSTN phone offer this feature. *P2P VoIP*, as construed here, offers only PC-to-PC communication and no PSTN interconnection. So in that sense, a pure Skype service is a case of *P2P VoIP*, while the SkypeOut and SkypeIn classify as *VoIP over Broadband*. The interconnection with PSTN is important since the PSTN switches are already CALEA compliant. This makes it possible to obtain call identifying information and content tracing of at least the PSTN end of a call.

Second is the question of the network and the service ownership. *VoIP in the Backbone* and *Facility-based VoIP* are vertically integrated business models, where the operator who owns the network and the service provider who bares the responsibility for the

service are the same. Conversely, for *VoIP over Broadband* and *P2P VoIP*, the operator and the service provider are different entities. This difference is important when carrying out content tracing upon a court order. Voice communication is achieved by two fundamental functions: "call signaling" that establishes and terminates a call and "bit transport" that carries bits of the actual voice conversation. In business models where the operator and the service provider are different entities, the call signaling function is carried out by the service provider, while the bit transport function is carried out by the operator (the network owner). When the court requires content tracing of a call, the service provider (carrying out call signaling function) knows the when the call originates and ends, while the operator has the capability to trace content. In this situation, the service provider and the operator, who compete for a customer under normal circumstances, must now collaborate to deliver the content trace.

The third is the of technology used to the end point. In *VoIP in the Backbone*, circuit-switching is used till the end device. In the rest of the business models, packet switching is used to connect the end points. This difference is important as the devices (phone or other devices such as PCs, PDAs etc.) used in *Facility-based VoIP, VoIP over Broadband,* or *P2P VoIP* have the potential for running the Internet Protocol (IP) stack on the devise, which makes them capable of running various encryption schemes. A user can now encrypt their voice traffic in ways that are difficult to tap and decrypt.

Recent regulatory intervention and the system of incentive

With the recent emphasis on homeland security, FCC, in response to FBI's petition, has sought to expand CALEA obligations to Internet, Broadband and VoIP service[5]. The FCC has concluded that VoIP services that Law Enforcement characterizes as "managed" or "mediated" are subject to CALEA as telecommunications carriers. Law Enforcement describes managed or mediated VoIP services as those services that offer voice communications calling capability whereby the VoIP provider acts as a mediator to manage the communication between its end points and to provide call set up, connection, termination, and party identification features, often generating or modifying dialing, signaling, switching, addressing or routing functions for the user. Law Enforcement distinguishes managed communications from "unmanaged" or "peer-to-peer" communications, which involve disintermediated communications that are set up and managed by the end user via its customer premises equipment or personal computer. In these non-managed, or disintermediated, communications, the VoIP provider has minimal or no involvement in the flow of packets during the communication, serving instead primarily as a directory that provides users' Internet web addresses to facilitate peer-to-peer communications.

Considering the classification of VoIP business models in Table 1, the CALEA and subsequent order suggests that the CALEA obligations are extended to the VoIP as shown in Table 2.

[5] FCC CALEA NPRM. ET Docket No. 04-295

Business Models Regulated under CALEA	Business Models not Regulated under CALEA
VoIP in the Backbone ***Facility-based VoIP*** ***VoIP over Broadband***	***P2P VoIP***

Table 2 Regulatory intent of extending CALEA to VoIP

The FCC has concluded that facilities-based providers of any type of broadband Internet access service,[6] whether provided on a wholesale or retail basis,[7] are subject to CALEA because they provide a replacement for a substantial portion of the local telephone exchange service used for dial-up Internet access service and treating such providers as telecommunications carriers for purposes of CALEA is in the public interest.[8] Broadband Internet access providers include, but are not limited to, wireline, cable modem, satellite, wireless, and broadband access via powerline companies.[9]

---

[6]*See* FCC CALEA NPRM. ET Docket No. 04-295. (defining "broadband Internet access service" for purposes of this proceeding). By "facilities-based," we mean entities that provide transmission or switching over their own facilities between the end user and the Internet Service Provider. We seek comment on this approach.

[7]We clarify that some entities that sell or lease mere transmission facilities on a non-common carrier basis, *e.g.*, dark fiber, bare space segment capacity or wireless spectrum, to other entities that use such transmission capacity to provide a broadband Internet access service, are not subject to CALEA under the Substantial Replacement Provision as broadband Internet access providers. Under such a scenario, the entity procuring the transmission capacity via the sale or lease and using it to provide broadband Internet access service (*e.g.*, a satellite earth station licensee) would be considered the facilities-based broadband Internet access service provider and thus, the entity subject to CALEA under the Substantial Replacement Provision.

[8]*See* Petition at 15-16, 23-28. We note that in other dockets, the Commission previously requested and received comment on the applicability of CALEA to wireline broadband Internet access service and has received comment on its applicability to cable modem service. *See Appropriate Framework for Broadband Access to the Internet over Wireline Facilities, Universal Service Obligations of Broadband Providers*, CC Docket No. 02-33, *Notice of Proposed Rulemaking*, 17 FCC Rcd 3019 (2002) (*Wireline Broadband NPRM*); *see also* FCC CALEA NPRM. ET Docket No. 04-295 (summarizing the fact that this proceeding encompasses the issue of the applicability of CALEA to wireline broadband Internet access previously raised in WC Docket No. 02-33); *Inquiry Concerning High-Speed Access to the Internet Over Cable and Other Facilities, Internet Over Cable Declaratory Ruling, Appropriate Regulatory Treatment for Broadband Access to the Internet Over Cable Facilities*, GN Docket No. 00-185 and CS Docket No. 02-52, *Declaratory Ruling and Notice of Proposed Rulemaking*, 17 FCC Rcd 4798 (2002) (*Cable Modem Declaratory Ruling & NPRM*), *aff'd in part, vacated in part, and remanded, Brand X Internet Services v. FCC*, 345 F.3d 1120 (9th Cir. 2003), stay granted pending cert. (April 9, 2004) (cable modem service constitutes the offering of both an information service and a telecommunications service to the end user). Parties that commented on CALEA issues in these dockets should respond to the instant docket.

[9]Broadband Internet access services are rapidly being developed or provided over technologies other than wireline and cable, such as wireless and powerline. For example, broadband Internet access service may be provided by CMRS carriers and fixed wireless companies such as local multipoint distribution service and 39 GHz licensees, or by wireless Internet Service Providers using unlicensed spectrum. *See, e.g., FCC Chairman Michael K. Powell announces Formation Of Wireless Broadband Access Task Force*, News Release (May 5, 2004); *Wireless Broadband Access Task Force Seeks Public Comment On Issues Related To Commission's Wireless Broadband Policies*, GN Docket No. 04-163, *Public Notice*, 19 FCC Rcd 8166 (2004). Broadband over powerline ("BPL") is a new technology being developed at a rapid pace to offer

Law Enforcement asserts that CALEA applies to broadband Internet access service and mediated VoIP services and that application is critical to its efforts to combat crime and terrorism.[10] The FCC bases its conclusion that the meaning of "telecommunications carrier" in CALEA is broader than its meaning under the Communications Act – and on Congress's stated intent "to preserve the government's ability, pursuant to court order or other lawful authorization, to intercept communications involving advanced technologies such as digital or wireless transmission modes."[11]

Incentive structure for various stakeholders

Now let us look at what kind of incentive structure the above intervention creates for different stakeholders. Balancing loop (B1 – Regulation of "managed" VoIP)[12] in Figure 1 shows the dynamics discussed in this paragraph. If we construe the total VoIP use to be made up of "managed" VoIP and P2P VoIP, as the use of VoIP goes up, the pressure to regulate builds up (the double bar indicate delay). The regulator hopes that the threat of regulation motivates the industry to collaborate to develop and deploy CALEA compliant technology. In our case, only the providers of "managed" VoIP should be expected to collaborate in compliance activities. Deployment of CALEA compliant technology increases the percentage of "managed" VoIP that is CALEA compliant, and over time, the pressure to regulate reduces.

---

voice and high-speed data capabilities. *See, e.g., Inquiry Regarding Carrier Current Systems, Including Broadband over Power Line Systems*, ET Docket No. 03-104, *Notice of Inquiry*, 18 FCC Rcd 8498 (2003) (seeking comment on technical issues relating to provision of BPL); *see also generally* United Power Line Council ("UPLC") Comments at 1-2.

[10] *See* Petition at 2, 25, 71; Law Enforcement Reply Comments at iii, 22.

[11] H.R. Rep. No. 103-827(I) (1994), *reprinted in* 1994 U.S.C.C.A.N. 3489 (*House Report*) (Summary and Purpose) (emphasis added); *see also* Petition at iii.

[12] Each arrow indicates a cause-effect relationship with the cause at the tail and the effect at the head of the arrow. The positive sign indicates a direct relationship between cause and effect. Increasing the cause increases the effect and decreasing the cause decreases the effect. The negative sign indicates an inverse relationship between the cause and the effect. Increasing the cause decreases the effect and decreasing the cause increases the effect. A balancing loop is where a change in any direction is counteracted by the resulting feedback. A reinforcing loop is where a change in any direction is exacerbated by the resulting feedback.

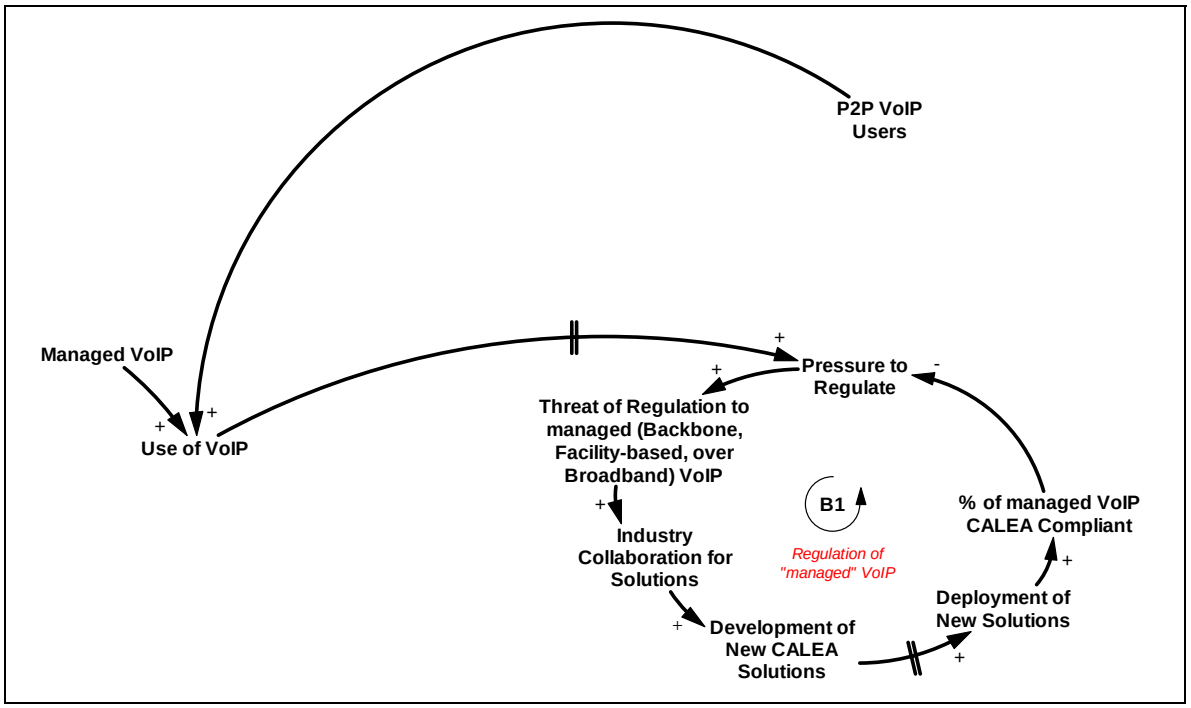


Figure 1 Use of VoIP and pressure to regulate

Incidentally, as the "managed" VoIP providers are required to comply with CALEA obligations, the new entrants in VoIP market find starting with "unmanaged" VoIP (in our classification *P2P VoIP*) more attractive. Reinforcing loop (R1 – Incentive to offer "unmanaged" (P2P) VoIP) in Figure 2 shows the dynamics discussed in this paragraph. The attractiveness of "unmanaged" VoIP is due to the cost of development and deployment of CALEA compliant technology, which small players may like to avoid. As more providers offer the "unmanaged" VoIP, its usage increases. This reduces the percentage of total VoIP that is CALEA compliant, something that should concern the regulator (particularly, the LEAs).

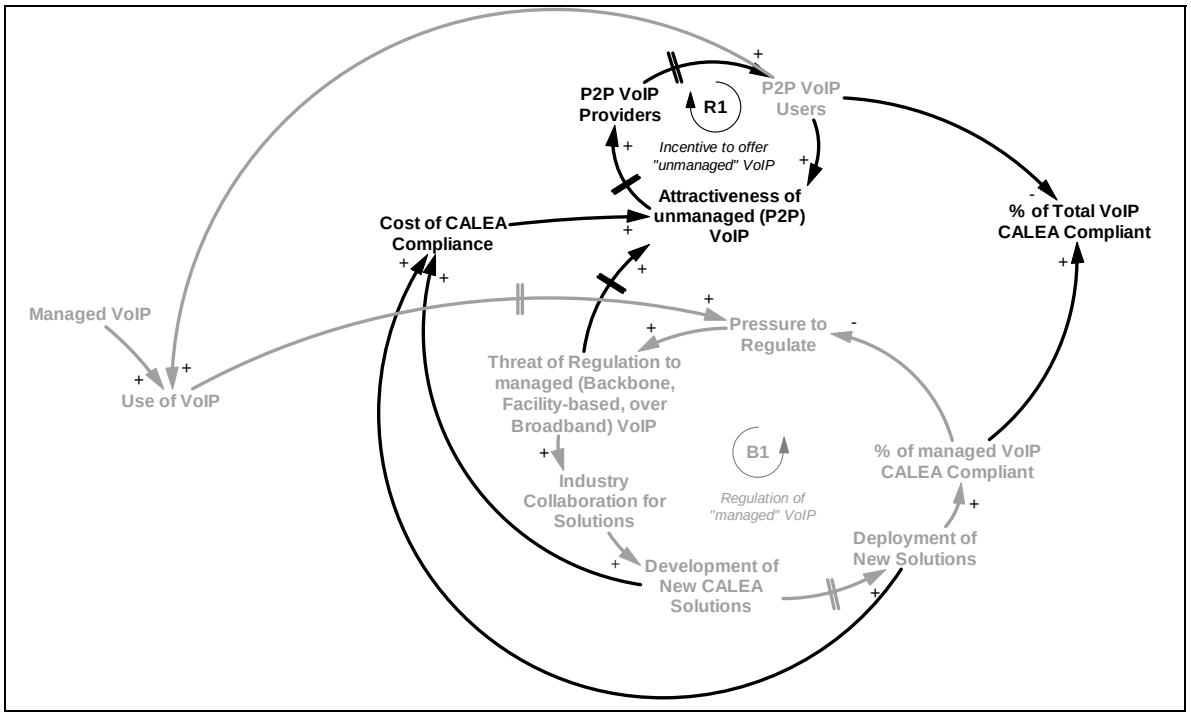


Figure 2 The incentive to offer "unmanaged" VoIP

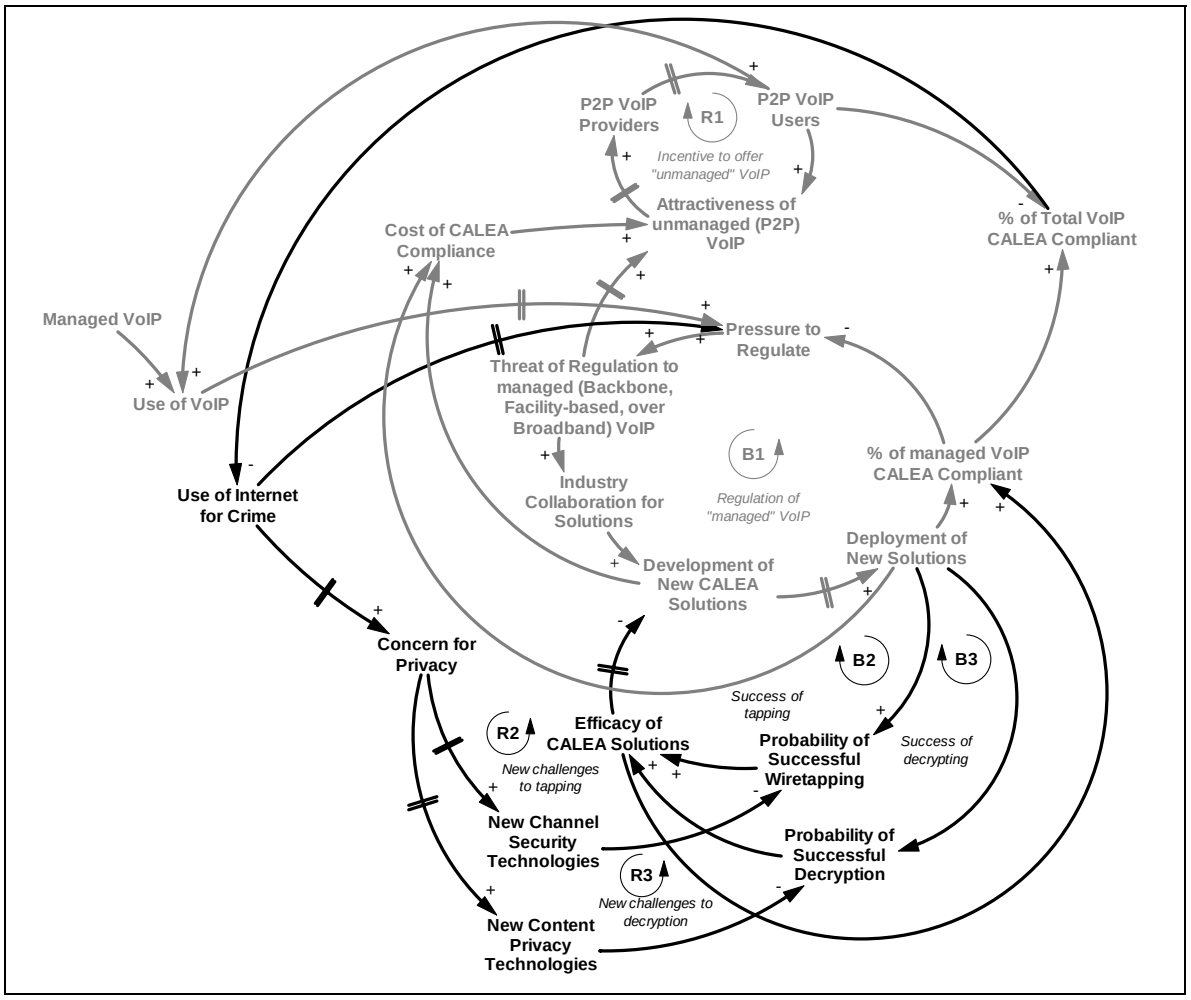


Figure 3 Regulatory compliance and the arms race with between criminals and the authority

The percentage of VoIP that can be tapped will determine how inclined is the criminal to use the Internet. The lower the CALEA compliance, the higher is the use of the non-compliant technology for crime, and vice versa. Please follow along Figure 3 for the rest of this paragraph. As the use of the Internet for crime rises, there are heightened concerns for privacy. If we construe the security as the security of the channel, and the privacy as the privacy of the content, new ways to encrypt the channel increases the channel security, while new ways to encrypt or desensitize the content increases privacy of the content. Here, we can see the potential for an arms race between criminals and the law enforcement. The deployment CALEA compliant technologies increase the efficacy of CALEA solutions in two ways: by increasing the probability of successful wiretap (B2-Success of tapping) and increasing the probability of decrypting the content once tapped (B3 – Success of decrypting). On the other hand, new ways to secure the channel (R2 – New challenges to tapping) and the content (R3 – New challenges to decryption) try to outpace the ability to tap and decrypt communications successfully.

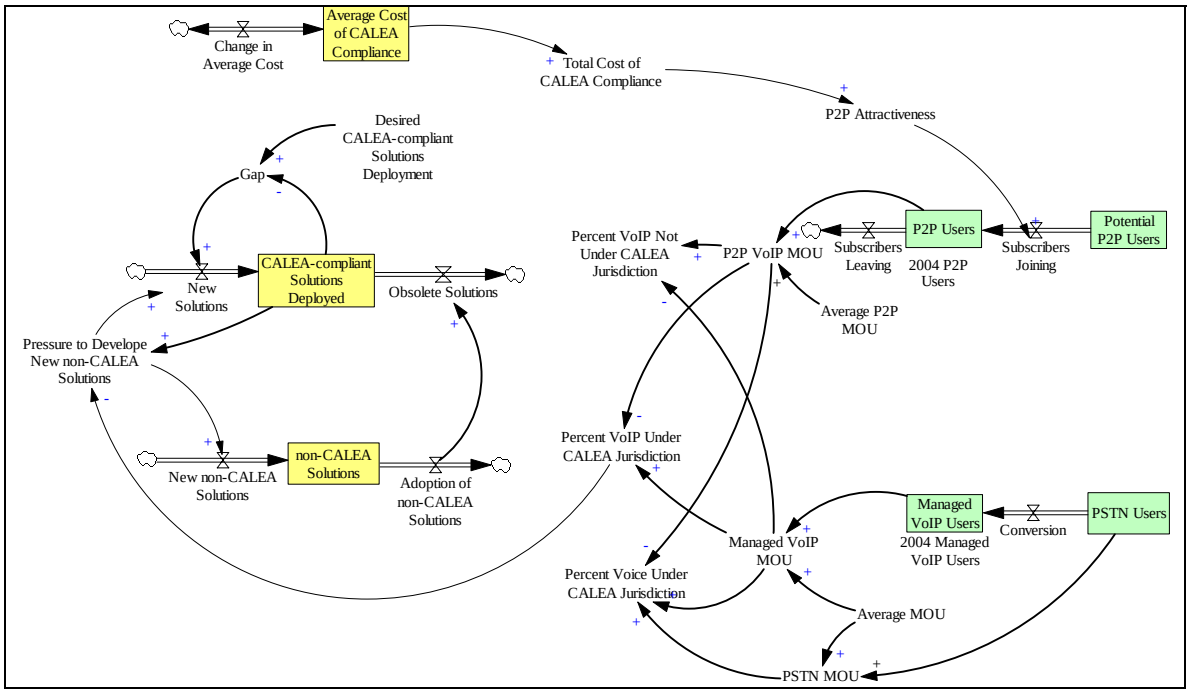


Figure 4 CALEA – a stylized computer model

Figure 4 shows a stylized version of the computer simulation of the CALEA model. For description of the complete working model, please refer to (Vaishnav 2005). Each box is like a bathtub with an inflow and an outflow; for example, the rate of deploying "New Solutions" fills up the "CALEA-compliant solutions deployed" tub, while the rate of "Obsolete Solutions" drains it. The adoption of "managed" and P2P VoIP are modeled as the Bass Diffusion Model (Bass, Krishnan et al. 1994). The PSTN users convert to the "managed" VoIP users, while the potential P2P users convert to the P2P users. We assume that any user can be a "managed" VoIP and a P2P VoIP user simultaneously, substituting a fraction of their traffic from "managed" to P2P. If the P2P VoIP usage increases, the percentage VoIP under CALEA jurisdiction reduces. This leads to regulatory pressure to develop CALEA solutions. New solutions are developed and deployed until the network meets the desired level of CALEA compliance. On one hand, deploying CALEA compliant solutions adds to the cost of CALEA compliance, while on the other, out of concern for security and privacy, it leads to development of new ways to secure the channel or content that is not CALEA compliant. The adoption of non-CALEA compliant solutions leads to making some of the already deployed CALEA compliant solutions obsolete.

Model parameterization and validation

Before we begin the analysis, let us discuss the parameterization and the basic validation of the model.

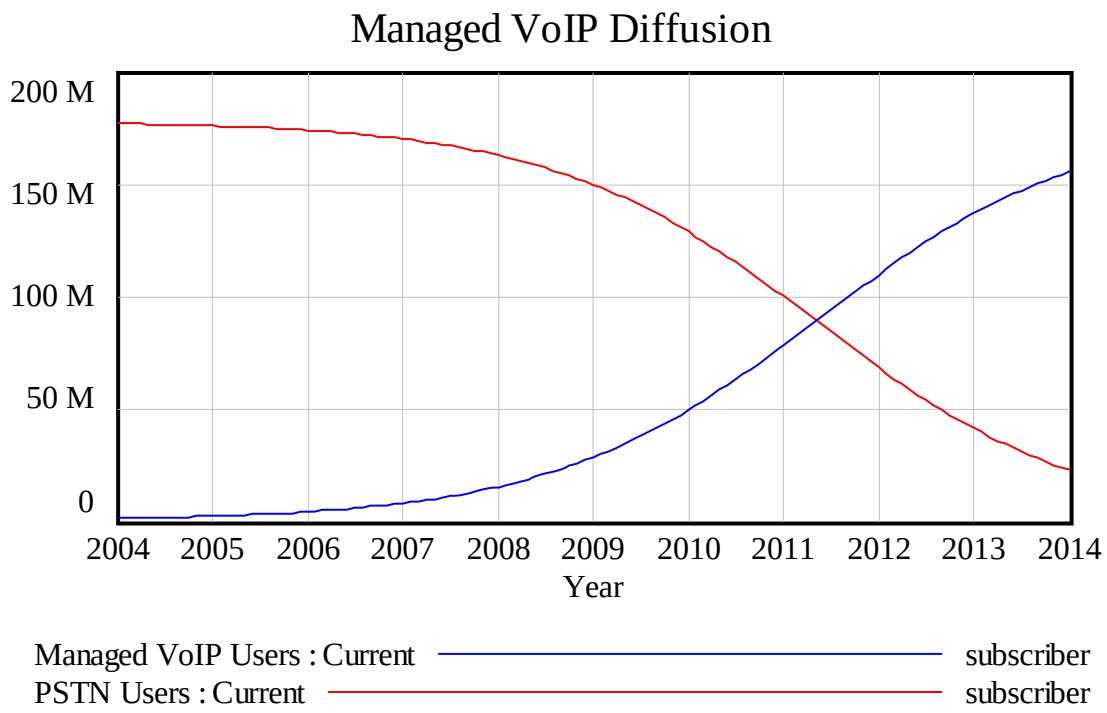


Figure 5 Managed VoIP Diffusion

Figure 5 shows the conversion of PSTN users into "managed" VoIP. The model parameters are set to match the number of "managed" VoIP users = 27 million by 2009, as forecasted by the International Data Corp ((IDC) 2005). This is the most optimistic forecast available for the "managed" VoIP diffusion. For a detailed list of model parameters, please refer to Table 6 of (Vaishnav 2005). According to this model, the crossover point between PSTN and "managed" VoIP Service users is between year 2011 and 2012.

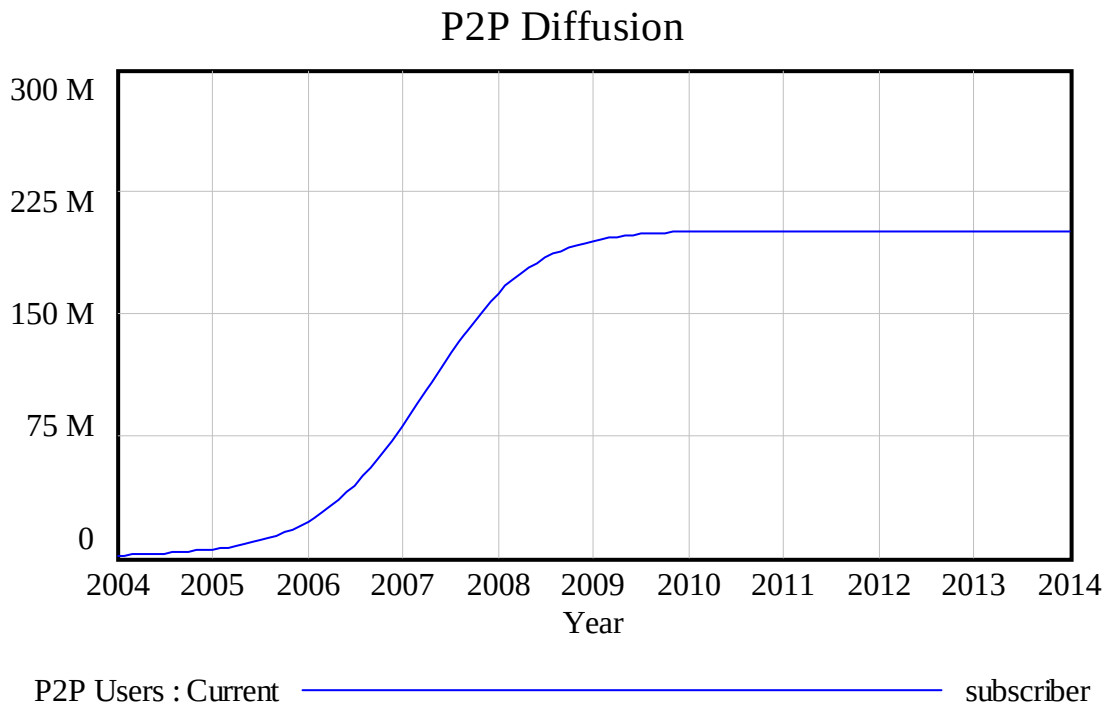


Figure 6 P2P Diffusion

Figure 6 shows diffusion of P2P users. Here, the parameters are set to match those of the "managed" VoIP part of the model. This assumption maybe arguable, but the reality is only worse! Because of Broadband proliferation and the availability of free application software, the P2P VoIP adoption, in reality, is faster than that of "managed" VoIP. So, in a way, our assumption is rather conservative. Comparing Figure 6 with Figure 5 shows that diffusion of P2P VoIP is quicker than that of "managed" VoIP. This is an artifact of the way the model is conceived. In our model, the adoption of P2P VoIP is accelerated by the rising cost of CALEA compliance. As one can see, both the adoptions follow an S-shaped growth.

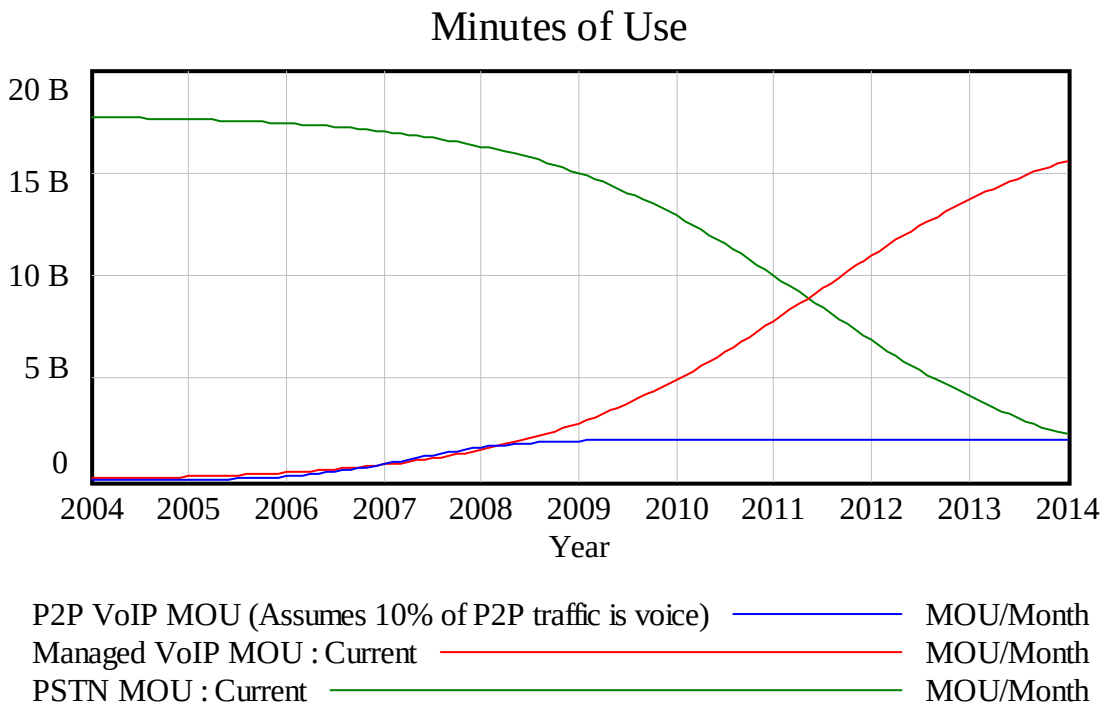


Figure 7 Minutes of Use

Figure 7 shows the minutes of use (MOU) for PSTN, managed VoIP and P2P VoIP. P2P VoIP MOU is only a fraction of the total VoIP because, in our model the P2P VoIP fraction is not allowed exceed to 0.1 (10%) of the total, once again to be conservative.

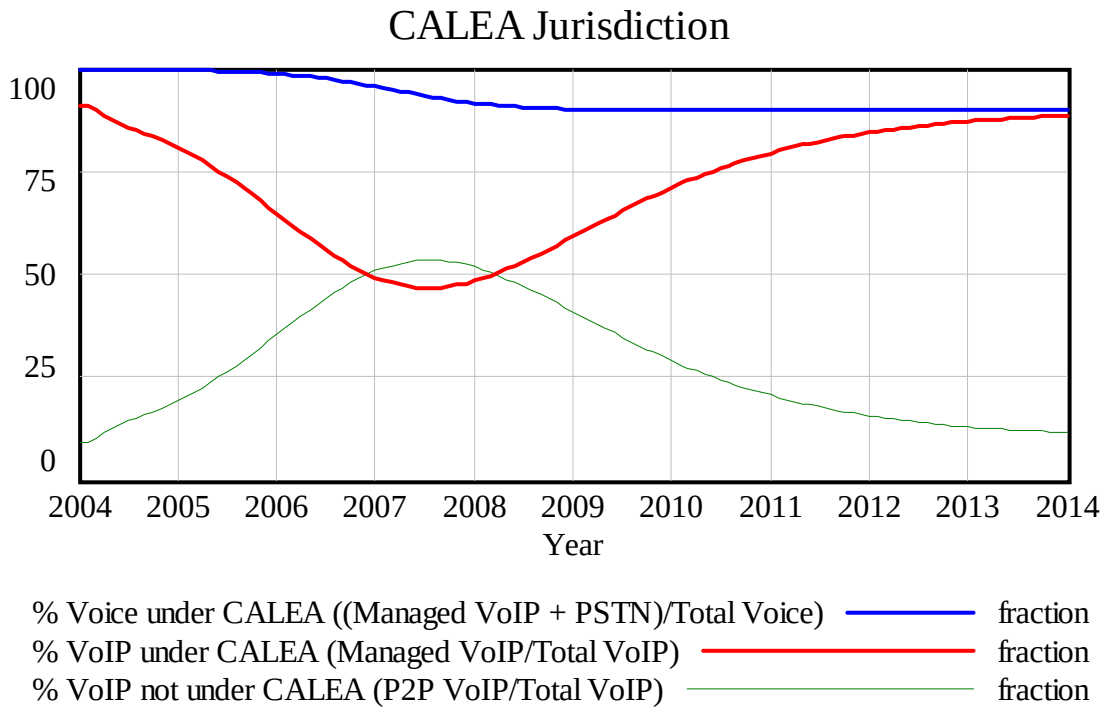


Figure 8 CALEA Jurisdiction

Figure 8 shows curves related to CALEA jurisdiction. % Voice under CALEA includes the PSTN and the "managed" VoIP fraction of the total voice MOU. From the validation point of view, the % voice traffic that is excluded from CALEA is limited to 10%, which is the upper limit we have set for the P2P VoIP fraction.

Policy Analysis and Lessons

Let us now turn to the policy lessons. There are two types of lessons drawn here. First, as shown in Figure 9, just the systems view of influences due to the recent CALEA intervention imparts some learning. Next, we augment this learning with some sensitivity analysis to demonstrate how difficult decision-making could be in such an environment.

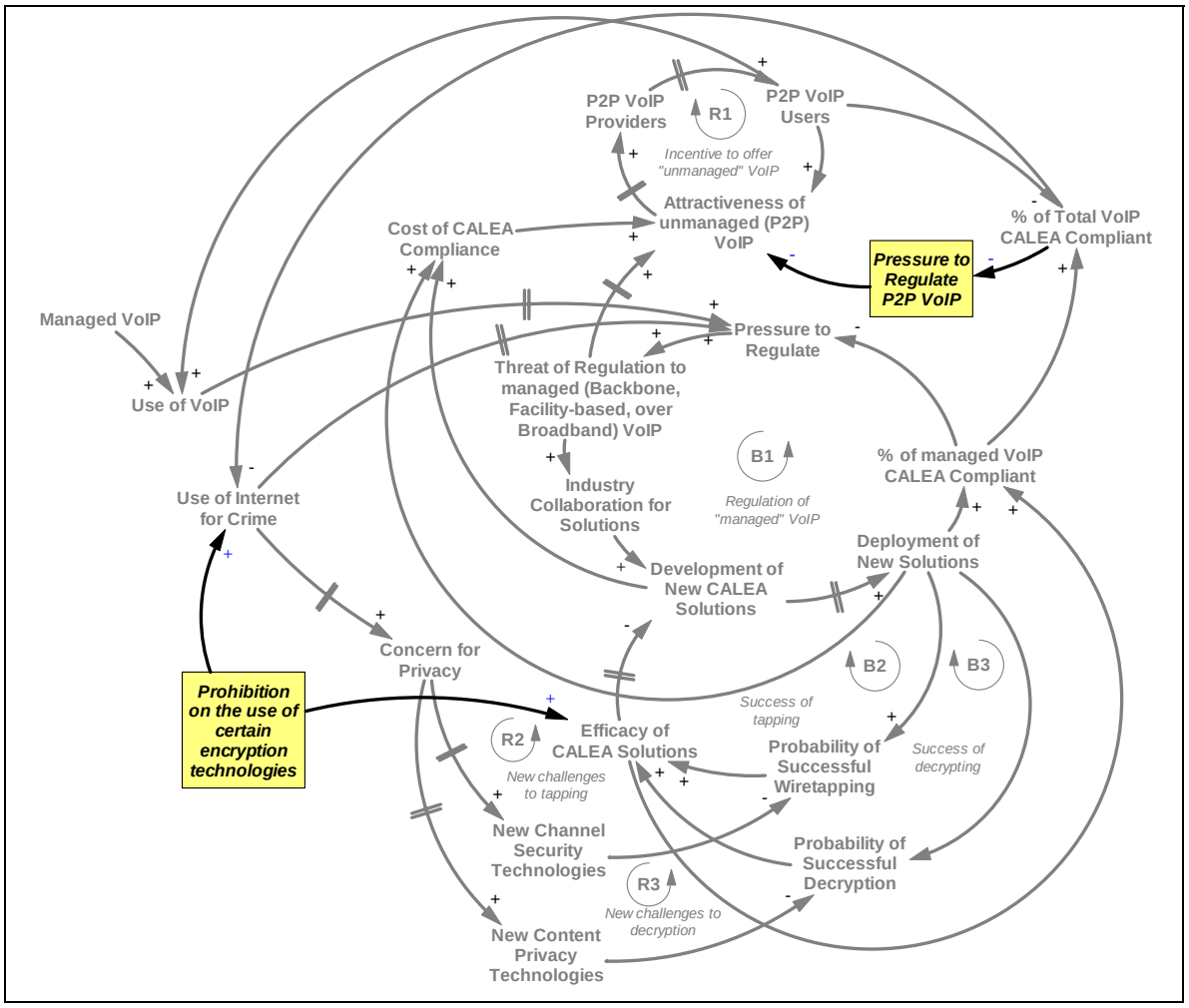


Figure 9 Policy levers and their impact

Policy Lesson 1: *Considering P2P a non-issue for CALEA is exactly what might make it an issue.*

In CALEA NPRM[13] and the subsequent order, the LEAs indicated and the FCC tentatively concluded that the P2P or the "unmanaged" VoIP should not be subject to CALEA. Currently, P2P VoIP may be exempt from CALEA as its share of total voice traffic is very small, it is technically harder to wiretap P2P traffic, and there is a tension

[13] FCC's CALEA NPRM. ET Docket No. 04-295, item 54, 55 and 57

between regulation and innovativeness. However, such an exemption expedites the need for regulating P2P VoIP under CALEA.

Diffusion of P2P VoIP reduces the % voice communications under CALEA jurisdiction. To examine the impact, we run the simulation multiple times, each time picking the upper limit for P2P VoIP fraction randomly between 5 – 20%, we see how P2P VoIP impacts % voice communications under CALEA as shown in Figure 10.

Figure 10(a) shows that when 20% of VoIP traffic is P2P, % voice under CALEA jurisdiction can be as low as 82%. In other words, 18% of voice traffic would be legally exempt from wiretapping.

Figure 10(b) and (c) show how % VoIP (alone) under CALEA jurisdiction is impacted. As high as 70% of VoIP traffic may be outside of the CALEA jurisdiction at one point, given the diffusion rates assumed in the model. Finally, Figure 10(d) shows how P2P VoIP diffusion, and the resulting pressure to increase CALEA compliance may drive the cost of CALEA compliance higher. This discussion leads us to our second lesson.

Policy Lesson 2: *If P2P VoIP aspires to become a telephony substitute, it will invite the threat of regulation.*

P2P VoIP experience has shown that there are no clear business models in this space when it comes to the question of making money. The only way any P2P VoIP provider has ever made money is to provide PSTN interconnection. However, under current statutory environment, the language and definitions of CALEA permit regulation of a voice service that interconnects with PSTN. So, interconnection with PSTN or a substitution of PSTN traffic is a way to invite regulation. Additionally, if substantial amount of telephony traffic is substituted with P2P voice, that offers further justification for social regulation such as CALEA and 911. Under such circumstances, the innovative freedom of the P2P technology would be kept unaffected only if the technology providers find ways to remain financially viable without aspiring to be a telephony substitutes.

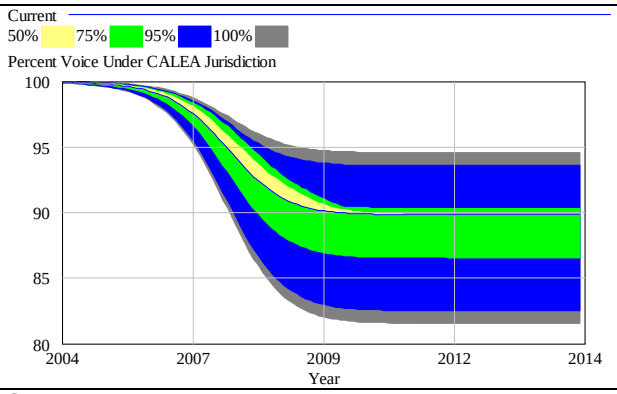
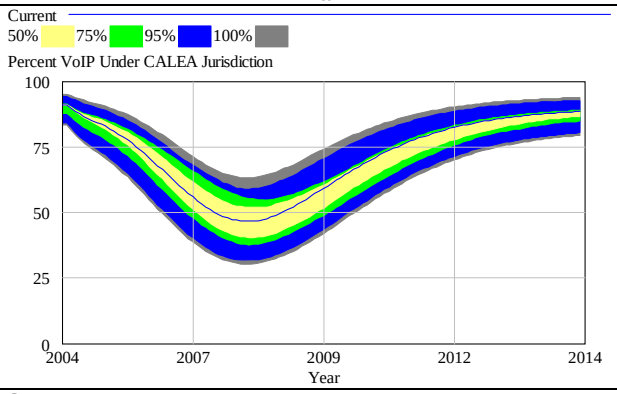
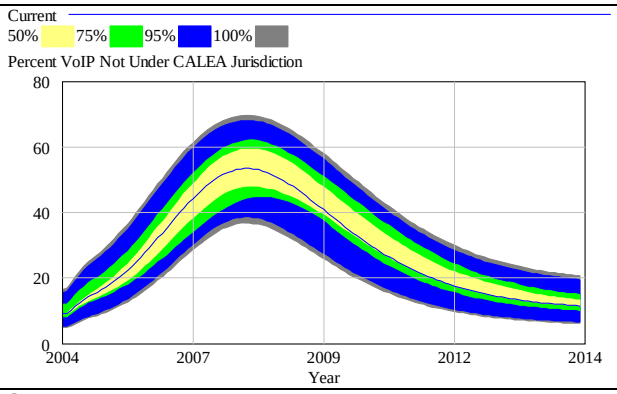
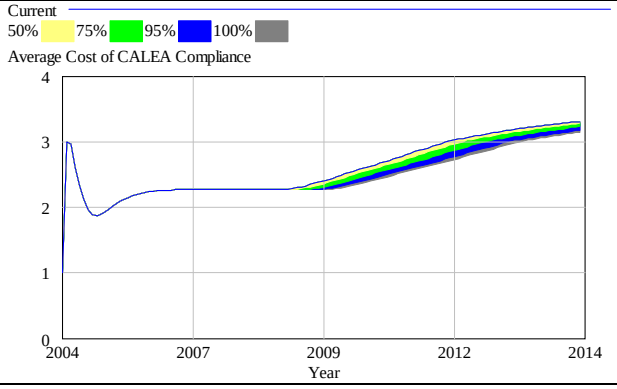
(a)	
(b)	
(c)	
(d)	

Figure 10 Sensitivity Analysis: Sensitivity of CALEA Jurisdiction and Compliance Cost to varying P2P and Managed VoIP Diffusion

Policy Lesson 3: *Arms race between CALEA-compliant and non-compliant technologies can raise the cost of compliance substantially.*

As the carriers deploy CALEA compliant technologies, various factors can lead to the use of non-compliant technologies. First, CALEA compliance may lag the technological progress in security and privacy technologies. Second, increase in concern for privacy may lead to proprietary privacy solutions. Finally, hackers and Internet-criminals may try to outsmart CALEA-compliant technologies. This arms race can raise the cost of CALEA compliance.

Figure 11 shows the sensitivity of CALEA compliance to the varying development and deployment rate of non-CALEA solutions. Here the develop rate and the adoption rate of the non-compliant technologies is varied uniformly between their normal rate and double the rate. Figure 11 shows that such a variance can raise the cost of CALEA compliance to as high as 4.5 times the normal cost.

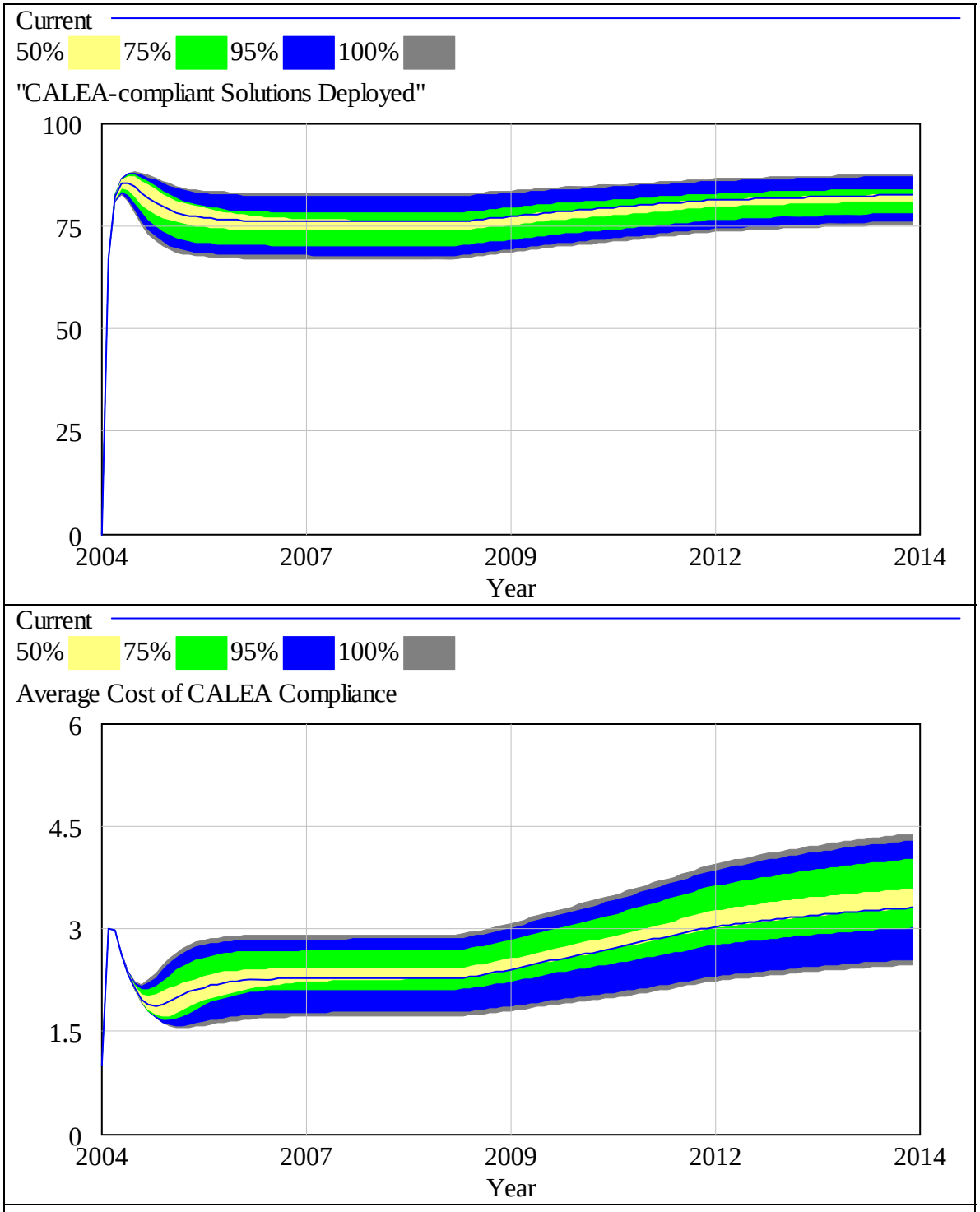


Figure 11 Sensitivity Analysis: Sensitivity of CALEA Deployment and Compliance Cost to varying Development and Deployment Rate of Non-CALEA Solutions

Policy Lesson 4: *Prohibiting the use of certain encryption techniques may help the LEA to keep their ability to wiretap intact; however, it also deprives the customers of the privacy the prohibited schemes would have offered, and thereby helps the Internet crime.*

If the use of new encryption scheme causes the CALEA compliance to lag behind, the tendency may be to prohibit the use of new encryption scheme until technology to wiretap it is developed. Use of stronger encryption schemes without the government approval has a history of inviting political wrath. However, banning the use of an encryption scheme, if only for a short time, may not be the best option. Internet-criminals could be interested in two aspects of wiretapping: they may want to avoid being wiretapped by the LEAs, and they may want to wiretap conversations to commit crime similar to the ones that currently happen through tapping phone conversations. Banning the use of an encryption scheme helps the LEAs by giving them the grace period to develop a mechanism to wiretap, but in the meanwhile it deprives customers of the privacy the use of the banned scheme would have offered, and helps criminal by leaving customers vulnerable to being wiretapped as a result of old encryption schemes. Figure 9 shows how this policy option affects the incentives.

Conclusion

In this paper we have demonstrated that the recent CALEA intervention resides in a complex socio-technical environment that can be analyzed as a feedback system. Analyzing the incentive structure the policy intervention creates for various stakeholders provides the first policy lessons. The next level of complexity can be tackled by sensitivity analysis done using computer simulation. Several policy lessons emerge as a result of our dynamic assessment of VoIP adoption, innovation and their interaction with new CALEA regulation. First, the current decision of exempting the unmanaged VoIP from CALEA obligations creates an incentive structure for its increased adoption. Second, if unmanaged VoIP aspires to be a telephony substitute, it will invite the threat of social regulation. Third, arms race between CALEA-compliant and non-compliant technologies can substantially raise the cost of CALEA compliance. Fourth, the LEA may choose to ban the use of certain encryption techniques to increase the ability to wiretap criminals; however, this would simultaneously reduce the consumer privacy protection and thereby the adoption of technology.

References

Bass, F. M., T. V. Krishnan, et al. (1994). "Why the Bass Model Fits without Decision Variables." Marketing Science 13(3): 203-223.
(IDC), I. D. C. (2005). Challenges with 911 to slow VoIP Adoption. Customer Relationship Management. 9: 14.
Vaishnav, C. (2005). Voice over Internet Protocol (VoIP): The Dynamics of Technology and Regulation. Technology and Policy Program, Massachusetts Institute of Technology Cambridge, USA.