Wiretapping the Internet: The Expansion of the Communications Assistance to Law Enforcement Act to Extend Government Surveillance

Christa M. Hibbard*

I. INTRODUCTION 372
II. HISTORY OF WIRETAP AND SURVEILLANCE LAW 374
III. PROPOSED EXPANSION OF CALEA 376
IV. GROWTH OF THE INTERNET AND THE RELATIONSHIP BETWEEN THE GOVERNMENT AND THE PRIVATE SECTOR ONLINE COMPANIES 377
A. History of the Relationship 378
B. Cooperation of the FBI and Online Companies 379
C. Compliance with CALEA 381
D. Implications of a Strong Relationship Between the Government and the Private Sector 382
V. CONCERNS OF INTERNET WIRETAPS IN THE FACE OF AN EXPANDING CALEA 383
A. Design of the Internet 383
B. Fourth Amendment Privacy Concerns 386
C. Threat to the First Amendment Freedom of Speech 388
D. Economic and Innovation Concerns 390

* J.D. Candidate, Indiana University Maurer School of Law, May 2012; B.A. in International Relations and Public Policy, William Smith College, 2009. The Author would like to thank Professor Fred Cate and the staff of the *Federal Communications Law Journal* for their assistance in the completion of this Note.

E. International Impact 391
VI. REASONS GIVEN FOR EXPANDING CALEA 392
A. Within Scope of Government Authority 392
B. Government Interest in Preventing and Investigating Crime 392
C. Current Retrofit Services Delay Ability to Wiretap 394
VII. MORE INFORMATION REQUIRED TO BALANCE COMPETING INTERESTS ADEQUATELY 395
A. Competing Interests 395
B. Lack of Information 396
C. Moving Forward 397
VIII. CONCLUSION 399

I. INTRODUCTION

As the Internet has become more prevalent over the past couple of decades, misuse of the Internet for criminal and terrorist activity has led American government officials to endeavor to improve their ability to deal with these threats. Criminal use of the Internet to take advantage of the government's limitations and circumvent traditional government phone wiretaps has inspired the Obama administration to create a task force led by officials from the Justice and Commerce Departments, the Federal Bureau of Investigation ("FBI"), and other agencies.[1] The goal of the task force is to expand the Communications Assistance to Law Enforcement Act ("CALEA"), which was passed in 1994 to regulate telephone and broadband companies to ensure compliance with standards "so that they can begin conducting surveillance of a target immediately after being presented with a court order."[2]

President Obama's task force intends to add provisions to CALEA that would allow the government to require "all services that enable communications – including encrypted e-mail transmitters like BlackBerry, social networking Web sites like Facebook and software that allows direct 'peer to peer' messaging like Skype – to be technically capable of complying if served with a wiretap order."[3] The expansion of CALEA would likely widen its scope to social networking sites, instant messaging,

---

1. *Wiretapping and Other Eavesdropping Devices and Methods*, N.Y. TIMES, Oct. 19, 2010, http://topics.nytimes.com/top/reference/timestopics/subjects/w/wiretapping_and_other_eavesdropping_devices_and_methods/index.html.

2. *Id.*; Communications Assistance to Law Enforcement Act, 47 U.S.C. § 1002 (2006).

3. Charlie Savage, *U.S. Tries to Make It Easier to Wiretap the Internet*, N.Y. TIMES, Sept. 27, 2010, http://www.nytimes.com/2010/09/27/us/27wiretap.html? pagewanted=all [hereinafter Savage Sept. 27].

gaming consoles that allow conversation among multiple players, and to word processing software that allows communication through Internet access.[4]

CALEA was first passed to require telephone and broadband companies to construct services that enable efficient and prompt compliance with wiretap orders. While the FCC has previously interpreted this 1994 version of CALEA to require compliance by communications over the Internet using Voice-over-Internet-Protocol ("VoIP") technology,[5] the expansion to all Internet communications would have significant consequences for the use of the Internet as we know it. The unique architecture of the Internet lends it to particular vulnerabilities with the consequence that an expansion of CALEA to all Internet communications would create problems regarding the innovative nature of the Internet as well as national security concerns. The proposed expansion of CALEA also raises free speech and privacy issues.

This Note will examine the competing interests related to expanding CALEA and will weigh the potential benefits and consequences of CALEA to conclude that substantially more information is needed to justify a change. Part II will give a background of wiretap and surveillance law, and establish the role of CALEA within the scope of this field of law. Part III will lay out the expansion proposal and the proposed requirements, in addition to discussing the reaction of online companies to the expansion thus far.

Part IV will discuss the relationship between the government and online companies. While the Internet was created by the U.S. government, this section will outline how once the Internet was beginning to be utilized by the public and other countries, the government allowed industry to take over primary control, while the government took a regulatory role. The status of this relationship has changed more recently, with a growing partnership between the government and the private sector. This section will discuss the potential implications of that development.

Part V will look at many of the arguments made against the expansion by opponents to the proposal. This examination will demonstrate that there are interests of the American public at stake. The CALEA expansion would likely have a negative impact on the use of the Internet as a means of

---

4. Laura W. Murphy & Christopher Calabrese, *Going Dark: Lawful Electronic Surveillance in the Face of New Technologies*, ACLU 3 (Feb. 17, 2011), http://www.aclu.org/files/assets/ACLU_Statement_for_the_Record_On_Proposed_Updates_to_the_Communications_Assistance_to_Law_Enforcement_Act_CALEA.pdf.

5. Susan Landau, *National Security on the Line*, 4 J. ON TELECOMM. & HIGH TECH. L. 409, 410 (2006).

communication, and would create the danger of chilling public speech. Another interest that will be discussed is the danger to Fourth Amendment privacy rights of Americans due to both the propensity of Internet users to reveal more information about themselves online, and the potential vulnerabilities of CALEA software, which could create the potential for access by third parties. The design of the Internet will also be discussed to demonstrate that the suggested change in CALEA would have implications for the Internet as it is currently structured, as well as national security concerns. This section will then discuss the potential economic and innovative issues which could arise, indicating that a change in the law would potentially have a negative impact on booming Internet industries. Part V will conclude by discussing the impact that the proposal would have internationally, both through the danger of any newly-developed software's use by foreign governments and the impact of the requirements of the law on foreign companies.

Part VI of this Note will then examine the counterarguments to these concerns, outlining the government interests behind the CALEA proposal. The government's argument that the expansion of the Act would not correlate to an expansion of government authority will first be examined, followed by a discussion of the government interest in preventing and investigating crime. The last section of Part VI will respond to national security arguments made against the proposal, arguing that current services to implement wiretaps retroactively have a greater likelihood of creating security holes for hackers than the proposed CALEA software.

Part VII will establish that in spite of relevant government interests advanced by the CALEA proposal, there is not enough information about why the government truly needs the services to justify the dangers that could arise. The potential costs are too great for the government to have free reign with expanding CALEA, and the FBI should either continue to use their powers under current wiretap laws to the best of their abilities, or give substantially more information to the American public about why such a change would be warranted. Even if the government presents further information about why such measures are needed, it is unlikely that the government interests will be found to outweigh the disadvantages to the American public. The FBI would then be recommended to proceed to the best of its abilities while utilizing its current capabilities.

II. HISTORY OF WIRETAP AND SURVEILLANCE LAW

Although the government has used wiretaps for law enforcement for over a century, Congress first regulated their use in the 1968 Omnibus

Crime Control and Safe Streets Act.[6] Title III of this Act permitted and closely regulated use of wiretaps for investigations of criminal activity, and Congress regulated government wiretapping in international investigations through the 1978 Foreign Intelligence Surveillance Act.[7] Over time, as technology has advanced, the law has similarly needed to change to stay relevant.

CALEA was passed in 1994 to require telephone and broadband companies to specifically construct their services to efficiently comply with wiretap orders.[8] The passing of CALEA represented a departure from previous wiretap law due to the government's use of its authority to establish the precise way that telephone networks should be designed.[9] As discussed further in Part IV, the legislation that ruled how communications providers would develop their networks demonstrates a growing relationship between the state and the private sector with regard to the Internet and wiretapping. According to Sun Microsystems Laboratories engineer Susan Landau, before CALEA, the government had "left the design of wiretap technology to the people who developed and ran the communications technology," rather than instructing communications providers on the specifics of how to configure their systems.[10]

As the market for traditional telephone systems began to decline with the advent of VoIP communications, the FBI found that it was unable to wiretap significant quantities of American telephonic communications and petitioned the FCC to interpret CALEA in a way which would expand it to include the authority of the government to regulate VoIP communications as well.[11] In 2004, the FCC complied with the FBI's request and controversially extended CALEA's power.[12] Much of the debate surrounding the FCC's decision to broaden CALEA had to do with the legitimacy of the FCC's power to interpret CALEA beyond what many believed the legislative intent entailed.[13] Critics had also questioned the FCC decision in light of the substantial threats that requiring wiretap capability would impose on innovation, privacy, and security.[14] Many of the concerns aired in response to the FCC's 2004 decision are still

---

6. *Id.* at 409.
7. *Id.* at 409–10.
8. *Wiretapping and Other Eavesdropping Devices and Methods*, *supra* note 1.
9. *See* Landau, *supra* note 5, at 417.
10. *Id.*; *see* Constance L. Martin, *Exalted Technology: Should CALEA Be Expanded to Authorize Internet Wiretapping?*, 32 RUTGERS COMPUTER & TECH. L.J. 140, 144–45 (2005).
11. Landau, *supra* note 5, at 410.
12. *Id.* at 421–22.
13. *See* Martin, *supra* note 10.
14. Landau, *supra* note 5, at 410.

substantially relevant and apply fully to the potential expansion of CALEA to all Internet communications.

The controversy surrounding the FCC's decision led to a D.C. Circuit Court case, which upheld the FCC's authority to interpret CALEA to include VoIP.[15] When the FCC interpreted CALEA to include VoIP, the rest of Internet communications were intentionally excluded as beyond the scope of the Act.[16] The contemporary expansion of CALEA that the Obama administration is promoting, in addition to creating new powers for law enforcement to wiretap communications over the Internet, would further endorse the FCC's interpretive power and endorse the use of wiretaps for VoIP communications.

III. PROPOSED EXPANSION OF CALEA

The amendment of CALEA to enable wiretapping of all Internet communications would likely involve an expansion of existing provisions that include specific changes that companies would need to make in order for their services to be wiretap-capable. Requirements for companies would potentially include:

- "Communications services that encrypt messages must have a way to unscramble them."[17]
- "Foreign-based providers that do business inside the United States must install a domestic office capable of performing intercepts."[18]
- "Developers of software that enables peer-to-peer communication must redesign their service to allow interception."[19]
- Provisions for a fine or penalty for failure to comply.[20]

In addition, CALEA would likely be amended to be written in "technologically neutral" terms to prevent its requirements from becoming obsolete.[21] These provisions would have consequences for the ability of the government to wiretap, the method in which Internet communications

---

15. Am. Council on Educ. v. FCC, 451 F.3d 226 (D.C. Cir. 2006).

16. Martin, *supra* note 10, at 155.

17. Savage Sept. 27, *supra* note 3; *see also* Charlie Savage, *FBI Seeks Wider Wiretap Law for Web*, N.Y. TIMES, Nov. 16, 2010, http://www.nytimes.com/2010/ 11/17/technology/ 17wiretap.html?_r=1&ref=wiretapping_and_other_eavesdropping_ devices_and_methods [hereinafter Savage Nov. 16].

18. Savage Sept. 27, *supra* note 3; Savage Nov. 16, *supra* note 17.

19. *Id*.

20. *Id.*

21. *Id.*

services run their organizations, and the privacy and freedom of speech of the American people.

In spite of the consequences that the expansion of CALEA would have, there was no public response from online companies after the Obama administration declared its intentions.[22] Companies such as Google, Facebook, Microsoft, Yahoo, and Research in Motion, who are "never shy about issuing press releases," were all silent in response to the plan.[23] The companies, which are normally strongly defensive of their privacy records and the privacy rights of their users, presented a front of silence, with the exception of Facebook's comment that "'[w]e will examine any proposal when and if it materializes but we can't comment on something we haven't seen. Generally, it's our policy to only comply with valid, legal requests for data."[24]

It has been speculated that the online companies have not responded to the declaration because the Obama administration has not offered specifics for the companies to comment on.[25] Yet the executives of a number of technology firms and Google and Facebook met with Robert S. Mueller III, the director of the FBI, on November 15, 2010, to discuss "a proposal to make it easier to wiretap Internet users."[26] The way the wiretap proposal was received was not clear as the online companies have not publicly discussed the matter, and it is, therefore, unknown what they would think about the potential expansion of CALEA.

IV. GROWTH OF THE INTERNET AND THE RELATIONSHIP BETWEEN THE GOVERNMENT AND THE PRIVATE SECTOR ONLINE COMPANIES

As is hinted by the meeting between the online companies and the FBI director regarding the expansion of wiretap capabilities to the Internet, the relationship between the private sector and the government has strengthened in the recent past with regard to the Internet. Although the authority to wiretap the Internet already exists, CALEA does not apply to online companies, and many of them wait until they are served with wiretap orders before developing interception capabilities.[27] The potential expansion of CALEA represents a trend of increased participation between

22. Verne G. Kopytoff, *Internet Wiretapping Proposal Met with Silence*, N.Y. TIMES BITS BLOG, Sept. 28, 2010, http://bits.blogs.nytimes.com/2010/09/28/internet-wiretapping-proposal-met-with-silence/.

23. *Id.*

24. *Id.*

25. *Id.*

26. Savage Nov. 16, *supra* note 17.

27. Savage Sept. 27, *supra* note 3.

the government and the private sector with regard to the Internet, which has potential adverse consequences.

A. History of the Relationship

While many view the Internet as a "grassroots" innovation, the Internet was originally created by American military strategists and was only later privatized.[28] In 1958, the United States Department of Defense created the Advanced Research Project Agency ("ARPA"), an agency to sponsor military research projects.[29] ARPA funded university and corporate programs "concerning the creation of a computer network to access and share data and programs among computers located in different places."[30] As the development of the project began during the Cold War, its appeal was that during large-scale international conflicts it could guarantee secure control over information transfers.[31] ARPANET, the precursor of the Internet, was designed by Massachusetts Institute of Technology researcher Lawrence G. Roberts in 1966.[32] In October 1969, the first "host-to-host message" was sent from the University of California at Los Angeles to the Stanford Research Institute, and, over time, nodes were added to expand the network.[33]

ARPANET's single network and few dozen nodes developed into the Internet over the course of a decade, becoming "a system of many interconnected networks, capable of almost indefinite expansion."[34] The Department of Defense initially continued to be heavily involved in the emergence of the Internet by "funding research and development, transferring technology to operational forces, using its financial resources to shape the commercial market for network products, and exercising management control over the ARPANET and its community of users."[35] While the government never truly released all of its relationship with the Internet, for a time it backed off controlling and running the Internet and

---

28. Michael D. Birnhack & Niva Elkin-Koren, *The Invisible Handshake: The Reemergence of the State in the Digital Environment*, 8 VA. J.L. & TECH. 6, paras. 2, 24 (2003).

29. ROMUALDO PASTOR-SATORRAS & ALESSANDRO VESPIGNANI, EVOLUTION AND STRUCTURE OF THE INTERNET: A STATISTICAL PHYSICS APPROACH xiii, 2 (2004).

30. *Id.* at 2.

31. *Id.*

32. *Id.* at 4.

33. *Id.*

34. JANET ABBATE, INVENTING THE INTERNET 113 (1999).

35. *Id.* at 114.

instead "focused on its regulatory role of shaping the rules that govern Internet-related activities."[36]

Not long after its government origins, the Internet was broadly viewed in the 1980s and 1990s as representing the decline of the State.[37] The Internet is a "decentralized network that derived its resilience from the absence of a central command," and many believed that control of it by a particular government would be unmanageable.[38] While the Internet was originally understood by some to be a "post-national situation" whose advent was confronted with "mourning or celebrating" the "inevitable sidelining of the State," the growing relationship between the government and online corporations suggests that this view is mistaken.[39]

In recent years, since the events of September 11, 2001, the U.S. government has started to reclaim some control over Internet operations through growing collaboration with private online companies.[40] Legislation was passed following the September 11th tragedy that increased the authority of the federal government to participate in the realm of the Internet, and the government has principally increased its power of electronic communication interception and collection.[41] Some argue that the government is regaining control by taking over "ready-made, often quite-centralized, private nodes of power" through both recruitment and, in many cases, voluntary action by the private companies.[42]

B. Cooperation of the FBI and Online Companies

The FBI has recently developed a "Going Dark Program" to improve its ability to perform electronic surveillance, particularly in light of what it says are difficulties in obtaining wiretap capabilities efficiently from some companies.[43] Under current systems, some communications carriers have been unable to carry out wiretap orders. One of the difficulties law enforcement has faced with Internet wiretapping is that one of the major American communications carriers failed to carry out over one hundred wiretap orders from 2008 to 2009 due to an eight-month lapse.[44] After the

---

36. Birnhack & Elkin-Koren, *supra* note 28, at para. 2.
37. *Id.* at para. 1.
38. *Id.* at paras. 1, 45.
39. *Id.* at para. 1.
40. *Id.* at para. 83.
41. *Id.* at paras. 83–84.
42. *Id.* at para. 2.
43. Savage Sept. 27, *supra* note 3; Charlie Savage, *Officials to Push to Bolster Law on Wiretapping*, N.Y. TIMES, Oct. 19, 2010, http://www.nytimes.com/2010/10/19/us/19wiretap.html [hereinafter Savage Oct. 19].
44. Savage Oct. 19, *supra* note 43.

first lapse was fixed, the carrier again experienced difficulties, which prevented electronic surveillance interception for another nine days.[45] In 2009, another major carrier dealt with similar interruptions "ranging from nine days to six weeks and was unable to comply with 14 wiretap orders."[46] Many of the interruptions were seen to be caused by upgrades made to networks, and the FBI sent engineers to help the companies address the problems.[47] Along with sending engineers to assist companies, every year the FBI spends around $20 million to assist private companies with fixing network problems that interfere with the FBI's electronic surveillance capabilities.[48]

In addition to FBI participation in network problems, further cooperation between the government and the private online companies has occurred through direct voluntary participation of companies with the government. Joseph E. Sullivan, Director of Compliance and Law Enforcement Relations at eBay, has "offered to hand over information, when requested, without a subpoena."[49] This is significant as the eBay corporation controls a colossal amount of information, including "financial records, names, user IDs and passwords, affiliations, e-mail addresses, physical addresses, shipping information, contact information, and transaction information" for eBay and PayPal.[50] Many other companies have adopted similar law enforcement-friendly policies, and have been met with similar responses: "[w]hether the Big Brother we distrust is government and its agencies, or multinational corporations, the emerging collaboration between the two in the online environment produces the ultimate threat."[51]

This sentiment has been echoed in testimony from the American Civil Liberties Union ("ACLU") submitted to the House Judiciary Subcommittee on Crime, Terrorism and Homeland Security on February 17, 2011, in an examination of the proposal of the CALEA expansion. The ACLU argued that the proposal would mean "a dramatic expansion of a dangerous idea" that the private sector and online companies would have the power to build the government's surveillance structure.[52]

---

45. *Id.*
46. *Id.*
47. *Id.*
48. *Id.*
49. Birnhack & Elkin-Koren, *supra* note 28, at para. 3.
50. *Id.*
51. *Id.*
52. Murphy & Calabrese, *supra* note 4, at 3.

C. Compliance with CALEA

Further development of the relationship between the government and the private sector online companies can be shown through the enactment of the "safe harbor" provision under CALEA. The current provision states that if a particular communications carrier meets industry standards, it will be considered in compliance.[53] The standard required includes "providing the content of a call or e-mail, along with identifying information like its recipient, time and location," and failure to meet this standard could lead to fines imposed by a judge or the FCC.[54] In spite of these strict standards, many law enforcement officials admit that "neither option is ever invoked" because the government prefers to foster the government relationship with industry rather than file complaints against companies.[55] The emphasis of the government on the industry relationship—rather than improving capabilities—can be argued to "create an incentive to let problems linger: Once a carrier's interception capability is restored -- even if it was fixed at taxpayer expense -- its service is compliant again with the 1994 law, so the issue is moot."[56]

Company compliance with the law has been rather difficult to establish in the first place, demonstrating the potential failures of CALEA to have beneficial results for law enforcement. When CALEA was originally enacted in 1994, compliance by telephone and communications carriers was so difficult that the FCC extended the original date for compliance by two years.[57] In spite of the extension, four years after the date set for compliance, there continued to be "frequent allegations of noncompliance."[58] There was a hearing House Subcommittee on Telecommunications and the Internet hearing in 2004 to discuss the lack of full CALEA implementation, during which "spokespersons for the FBI and DOJ stated that many companies still do not comply with CALEA, primarily because of inadequate technology."[59]

In a Department of Justice audit report, it has also been noted that the costs of implementation had been much higher than estimated, and it was significant that "the FBI could not show the extent to which inability to

---

53. Communications Assistance to Law Enforcement Act, 47 U.S.C. § 1002 (2006); *see Wiretapping and Other Eavesdropping Devices and Methods*, *supra* note 1.

54. *Wiretapping and Other Eavesdropping Devises and Methods*, *supra* note 1.

55. *Id.*

56. Savage Oct. 19, *supra* note 43.

57. Martin, *supra* note 10, at 145–46.

58. *Id.* at 146.

59. *Id.* at 146 n.35.

implement CALEA had negatively affected FBI surveillance."[60] The goal of compliance was unsuccessful in spite of the $500 million authorized by CALEA for reasonable cost reimbursement for carriers and the threat of a fine for each noncomplying carrier of up to $10,000 each.[61] The difficulties faced by companies attempting to achieve compliance raises questions as to whether government-required system changes are the most effective method for law enforcement to increase their ability to wiretap suspects that are Internet users.

D. Implications of a Strong Relationship Between the Government and the Private Sector

While a strengthened relationship between the government and private industry with regard to the Internet could potentially be the answer to solving compliance problems with wiretap orders, this relationship also poses a threat to American industry. The development of CALEA was a departure from previous law due to its requirement that companies follow government-directed approaches to configure their networks to comply with wiretap orders. The growth of the government-industry collaboration, signified by this change, could pose a danger to the online environment,[62] both as a threat to individual freedom and as an unwelcome influence on the development of technology and code.[63]

Landau argues that the deviation from previous law that CALEA represents is problematic due to the imposition on providers of a plan for how technical networks should work. Landau points out that "[i]n no instance prior to CALEA did Congress legislate how the communications providers should configure their networks; instead, Congress left the design of wiretap technology to the people who developed and ran the communications technology."[64] Landau also argues that it would make more sense to leave the discretion about network configuration to the providers themselves in order to best balance the needs of law enforcement and the privacy needs of customers through use of market forces.[65] The existence of market forces put communications carriers "in a natural position to balance the opposing needs of law enforcement and customer

60. Martin, *supra* note 10, at 146 n.34 (citation omitted).
61. *Id.* at 145–46.
62. Birnhack & Elkin-Koren, *supra* note 28, at para. 3.
63. *Id.* at paras. 20–21.
64. Landau, *supra* note 5, at 417.
65. *See id.*

privacy," and the industry itself should therefore be in charge of how networks are configured to comply with CALEA.[66]

V. CONCERNS OF INTERNET WIRETAPS IN THE FACE OF AN EXPANDING CALEA

In addition to reservations about the application of current CALEA law and the consequences of the relationship between the government and the private sector, there are similar concerns about the expansion of CALEA and the ramifications it would have for American citizens, online communications providers, and the Internet. Such fears have to do with concerns about CALEA's impact on the First Amendment right to freedom of speech and the Fourth Amendment right to privacy, as well as whether CALEA's implementation would affect national security. There are also potential issues regarding the Internet's economic impact and whether its innovative powers would be adversely altered by CALEA software. The final concern in the face of CALEA is the impact it would have internationally, both on citizens of other countries and on foreign corporations. Due to the nature of these concerns, the government should provide more information and evaluate the competing interests at hand in order to best serve the American public.

A. Design of the Internet

The structure of the Internet raises relevant concerns due to the impact that allowing the installation of access points would have on the Internet itself. James X. Dempsey, Vice President of the Center for Democracy and Technology, argues that the CALEA proposal would have "'huge implications' and challenge[] 'fundamental elements of the Internet revolution' – including its decentralized design."[67] The "hub-and-spoke" design of phone and broadband communication contrasts strongly with the decentralized design of the Internet, meaning that there could be serious consequences in attempts to require wiretap technology for the Internet.[68] If "requiring Internet providers to be able to unscramble encrypted messages or intercept any transmitted communication also calls for them to function like centralized carriers, the shift will reverse what made the Internet – and made it a fount of economic growth."[69] The expansion of CALEA could,

66. *Id.*

67. Savage Sept. 27, *supra* note 3.

68. Editorial, *Major Technical Difficulties*, N.Y. TIMES, Nov. 2, 2010, http://www.nytimes.com/2010/11/03/opinion/03wed1.html.

69. *Id.*

therefore, have significant ramifications for the structure of the Internet in general.

Substantially different than the hub-and-spoke design of phone and broadband, the Internet is a "packet-switched" network.[70] This means that there are no fixed circuits created as pathways for a particular communication and the data is instead divided into packets to be communicated.[71] Each individual packet then travels via the least-congested route to later be reassembled at the other end.[72] This frequently means that the packets travel together, but sometimes the packets are separated during transit.[73] As the system is created to allow packets to travel separately, it would be increasingly difficult for a wiretap system to intercept the information anywhere other than at the endpoints.[74] According to Landau, the design of the Internet means that "'unless the communication is tapped at the endpoints . . . it's impossible to guarantee 100 percent access to all communication packets."[75] Wiretaps on a traditional Public Switch Telephone Network create switches somewhere between each end, but the structure of the Internet therefore requires a different approach for an effective wiretap.[76] An additional problem is that "[a]s the choke point for communications comes closer to the source of the communications, the risk of detection becomes greater."[77] CALEA wiretaps thus far have required that their providers ensure that their information be sent over a specific switch somewhere in the middle for government access.[78] As it is difficult to guarantee access to all information unless the wiretap is at the endpoint of a communication, traditional wiretaps may be unable to obtain sought-after information.

The architecture of the Internet also lends itself to vulnerabilities and makes it more difficult to wiretap. Professor Steven Bellovin of Columbia University argues that the proposed expansion would require a different and more complicated protocol, which would create serious security

---

70. Landau, *supra* note 5, at 424.

71. *Id.*

72. *Id.*

73. *Id.*

74. *See* Gene D. Park, Note, *Internet Wiretaps: Applying the Communications Assistance for Law Enforcement Act to Broadband Services*, 2 J.L. & POL'Y FOR INFO. SOC'Y 599, 615 (2006).

75. *Id.* (footnote omitted).

76. Timothy Singleton, *Big Brother Hears You, but Can He Understand What He Hears? The Problematic Application of CALEA to VoIP Communications in the Age of Encryption*, 15 TULSA J. COMP. & INT'L L. 283, 286–88 (2008).

77. *Id.* at 307.

78. *Id.* at 288.

problems.[79] The Internet is easier to undermine than a telephone network due to its "flexibility and dynamism," and creating access points within the Internet would "build security vulnerabilities into the communication protocols."[80] Professor Bellovin stated that "many previous attempts to add such features have resulted in new, easily exploited security flaws rather than better law enforcement access."[81]

There is also little proof that software creating access points would be safeguarded against abuse.[82] As a Greek form of wiretapping that similarly created online access points was previously exploited, creating a significant threat to national security, it appears that the fears of those opposing CALEA may have valid foundations. In 2005, hackers broke through a Greek legally-mandated wiretap function to gain access to communications of government officials.[83] It was eventually discovered that over "100 high-ranking government officials and dignitaries including the prime minister of Greece, his wife, and the Mayor of Athens" had their phones compromised and conversations overheard through manipulation of the Vodafone Greece network.[84] The bugging began sometime before the 2004 Olympic Games in Athens and remained undiscovered until January 24, 2005.[85] Not only is it worrisome that the hackers remained undiscovered for so long, but even more concerning is that the only reason they were ever discovered at all was that the hackers added something to the software that blocked delivery of text messages, leading technicians to check if anyone was listening in the "electronic back door."[86] The scope of the information obtained by the hackers and what it was used for was never discovered, but "no other computer crime on record has had the same potential for capturing information about affairs of state."[87]

The American system would have similar vulnerabilities if wiretap capabilities were inserted into the networks of communications carriers, and it has been specifically alleged that retrofitted "CALEA installations are poorly maintained, lacking adequate security measures such as a

---

79. Murphy & Calabrese, *supra* note 4, at 5.

80. Landau, *supra* note 5, at 426.

81. Murphy & Calabrese, *supra* note 4, at 5.

82. John Markoff, *Engineers as Counterspies: How the Greek Cellphone System Was Bugged*, N.Y. TIMES BITS BLOG (July 10, 2007, 7:40 AM), http://bits.blogs.nytimes.com/2007/07/10/engineers-as-counterspys-how-the-greek-cellphone-system-was-bugged/.

83. Savage Sept. 27, *supra* note 3.

84. Markoff, *supra* note 82.

85. Vassilis Prevelakis & Diomidis Spinellis, *The Athens Affair*, IEEE SPECTRUM (July 2007), http://spectrum.ieee.org/telecom/security/the-athens-affair.

86. Markoff, *supra* note 82.

87. Prevelakis & Spinellis, *supra* note 85.

firewall, and are open to hacking."[88] There are also potential security risks with Internet wiretapping because the packets of information obtained through Internet wiretapping are then shipped via the Internet to a third party.[89] This system would allow an insider the access and capability to retrieve unauthorized information without being discovered.[90]

The possibility that building an access point for the FBI to wiretap communications might also be a weakness for hackers to exploit is a potential national security problem.[91] Landau argues that this technology "presents a fat target for foreign intelligence agencies," giving them the capability of broad access to American Internet communications without needing to build any access points of their own.[92] She says that "[w]ere Internet wiretapping technology to be penetrated and exploited by foreign intelligence services, massive surveillance of U.S. 'persons' (citizens and corporations) might follow."[93] This level of potential breach could be devastating for the well-being of American corporations as well as the safety of American citizens.

B. Fourth Amendment Privacy Concerns

Beyond traditional concerns with law enforcement wiretapping, the implementation of Internet wiretaps poses additional privacy considerations. The expansion of CALEA would not change the government's capabilities of obtaining warrants under existing wiretap law, but privacy interests would still be threatened through the creation of "access points" by law enforcement.[94] Much of the additional concern for application of wiretaps to the Internet has to do with the particularities of the Internet that would make it possible for a third party to find access to private information through the access points.[95] The Internet's decentralized and open features combined with the fact that it involves distribution of data packets over networks "presents difficulties in isolating specific communications directed for extraction under a court order."[96] Access points created to enable law enforcement to wiretap the Internet could very possibly "also allow unauthorized access into private

88. Park, *supra* note 74, at 619 (citation omitted).
89. Landau, *supra* note 5, at 432.
90. *Id.*
91. Martin, *supra* note 10, at 176.
92. Landau, *supra* note 5, at 432–33.
93. *Id.* at 433.
94. Park, *supra* note 74, at 613.
95. *Id.* at 603.
96. *Id.*

communications."[97] This privacy concern was also an issue with the expansion of CALEA by the FCC to apply to VoIP communications, but it is even more relevant to a potential decision to expand easy access for wiretap capabilities to all Internet communications.

The concerns of allowing easy access points over the Internet for all online communications companies instills further concern due to the fact that people reveal more of themselves online than over telephone conversations.[98] Privacy advocates argue that the Internet should be subject to different treatment than phone networks due to the fact that the Internet provides an entirely different medium of communication.[99] Susan Freiwald, Professor at the University of San Francisco School of Law, argues:

> [W]e reveal more of ourselves online than on the telephone, because we are more clearly identified with our Internet activities via our password-protected accounts. We transmit much richer information online than offline; in addition to conversations, we send pictures, videos, songs, and long documents. We also create records of our activities when we shop, read, play, organize, and date online.[100]

As Freiwald's argument demonstrates, average Americans reveal more of themselves online because the medium allows for a variety of different types of communication. The risk is, therefore, that the government will have access to substantially more information than it would with a telephone wiretap. As pointed out by Democratic Senator Ron Wyden of Oregon in response to the FCC's expansive interpretation of CALEA, "[i]t's possible to fight terrorism ferociously without gutting civil liberties. The challenge in striking that balance is to have ground rules."[101]

Fears surrounding Americans' privacy concerns regarding unauthorized wiretaps have been validated by previous government action. The Bush administration amended the Foreign Intelligence Surveillance Act ("FISA") in 2008, which "sanctioned spying without a warrant, without suspicion, and without court approval."[102] The law was amended in order to retroactively give legal cover to over five years of spying through illegal wiretaps by the government.[103] While the expansion of CALEA is not for a similar retroactive protection, "the risks of executive overreach

---

97. *Id.*

98. *Id.* at 613 (citing Susan Friewald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9, 77 (2004)).

99. *Id.*

100. *Id.*

101. Martin, *supra* note 10, at 180.

102. Editorial, *supra* note 68.

103. *Id.*

are still there."[104] The argument has been made that Congress should be especially careful in drafting any new provisions for CALEA in order to delineate what powers are given to the executive branch, such that the scope of the law will not "spread far beyond what's said to be contemplated."[105]

Additional privacy concerns exist due to the Supreme Court decision in *Bartnicki v. Vopper*, which indicates that newspapers and publishers can, in some situations, escape criminal liability that would otherwise arise from publishing illegally intercepted conversations.[106] The Supreme Court held that "privacy concerns give way when balanced against the interest in publishing matters of public importance."[107] As Internet wiretaps provide vulnerabilities, which could be taken advantage of by third parties, the ability of the media to potentially publish material obtained illegally without facing government sanctions further heightens this threat to American privacy.

A privacy advocacy group, the Electronic Frontier Foundation, is concerned that there are "obvious civil liberty and privacy issues" with the Obama administration plan to expand CALEA.[108] It argues that the existing statutes for wiretap orders give law enforcement agencies sufficient reign to have access to Internet communication information.[109] It also argues that the reason for the expansion of the law is that the government does not get the information as quickly as it would wish, and that the government should have to "bear the burden of proof for why [the government] need[s] this," although in most circumstances it tends not to be required.[110] The Obama administration should therefore provide more information to justify such threats to Americans' rights.

C. Threat to the First Amendment Freedom of Speech

Among the extensive concerns regarding application of CALEA to all Internet companies is the potential threat to speech it would impose. Privacy advocates argue that the plan would be a threat to First Amendment freedom of speech protections and that the installation of wiretap capabilities within Internet communications provider networks

104. *Id.*
105. *Id.*
106. 532 U.S. 514 (2001).
107. *Id.* at 534.
108. Kopytoff, *supra* note 22.
109. *Id.*
110. *Id.*

would be readily open to abuse.[111] Due to the potential for abuse of the proposed wiretap capabilities, there is an inherent fear that chilling of speech could occur.

There are two types of chilling effects: one that chills illegal conduct when a government policy or statute prohibits it, and one "when individuals seeking to engage in lawful activity are deterred from doing so by a government regulation not specifically directed at that activity."[112] This second form of chilling effect is extremely harmful to both the individual deterred from exercising his or her rights and to society in general.[113] The First Amendment has been considered to be "based on the assumption, perhaps unprovable, that the uninhibited exchange of information, the active search for truth, and the open criticism of government are positive virtues."[114] Some argue that the level of impact of the chilling effect depends on the fear associated with the potential chilling.[115] In the case of Internet wiretaps, the fear that private information communicated to other parties could be intercepted by the government or hackers could cause pervasive anxiety.

The interference with online speech is alarming due to the immense benefits provided by anonymity in particular. The Supreme Court has said that protections for anonymous speech epitomize the purpose behind the First Amendment: "to protect unpopular individuals from retaliation—and their ideas from suppression—at the hand of an intolerant society."[116] In some cases, anonymity on the Internet is critical due to the sensitive nature of material being shared by online speakers such as whistleblowers and human rights workers struggling against repressive regimes.[117] The Internet is touted for its propensity to allow people to interact online anonymously and to encourage people to be able to say anything they wish without fear of repercussion.[118] It has also been described as "one of the greatest tools for exercising an individual's constitutional rights."[119] If CALEA is amended, people will feel less secure in the anonymity of online forums

---

111. *Id.*

112. Gayle Horn, Note, *Online Searches and Offline Challenges: The Chilling Effect, Anonymity and the New FBI Guidelines*, 60 N.Y.U. ANN. SURV. AM. L. 735, 749 (2005).

113. *Id.* at 749–50.

114. *Id.* at 750 (quoting Frederick Schauer, *Fear, Risk and The First Amendment: Unraveling the 'Chilling Effect*,*'* 58 B.U. L. REV. 685, 693 (1978)).

115. *Id.*

116. McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 357 (1995).

117. *Anonymity*, ELECTRONIC FRONTIER FOUNDATION, http://www.eff.org/issues/anonymity (last visited Feb. 20, 2012).

118. *Id*.; *see also* Murphy & Calabrese, *supra* note 4, at 4.

119. Murphy & Calabrese, *supra* note 4, at 4.

and online communication, and the abundant flow of speech on the Internet could be chilled.

Those who argue against an anonymous Internet point out that online anonymity creates opportunities for crime and harassment to go unpunished.[120] Anonymity is sometimes said to allow people to avoid taking responsibility for their communications and to encourage things like "offensive or defamatory newsgroup postings, or sexually harassing e-mail."[121] Although anonymity has been blamed for allowing anonymous speakers to be "hit-and-run drivers on the infobahn,"[122] the disadvantages caused by its abuse do not outweigh its significant benefits.

D. Economic and Innovation Concerns

There are concerns with regard to the well-being of industry and the innovation of online companies related to the CALEA proposal. One of the first issues is that much of the cost would be covered by the online companies themselves. According to former Justice Department lawyer Michael A. Sussmann, the CALEA expansion proposal would lead to a "technology and security headache" because of the hassles of implementation, and "the investigative burden and costs will shift to providers."[123]

There is also evidence that the consequential implementation of the proposal would discourage innovation and impede production. Landau argued that the proposal would be particularly detrimental to small startups, as "[e]very engineer who is developing the wiretap system is an engineer who is not building in greater security, more features, or getting the product out faster."[124] The fear that the proposal will interfere with innovation of online companies is similarly shared by a number of other critics, as well as the Departments of Commerce and State.[125] When the FCC initially interpreted CALEA to expand its scope beyond how it had been used to apply to VoIP, there was speculation that the FCC would institute a pre-approval system for technology, "requiring submission to and approval by the FCC."[126] Although the request was not granted for the system at the time, the implementation of Internet wiretaps would impose a hindrance on

---

120. George P. Long, III, *Who Are You?: Identity and Anonymity in Cyberspace*, 55 U. PITT. L. REV. 1177, 1179 (1994).

121. Lee Tien, *Who's Afraid of Anonymous Speech?* McIntyre *and the Internet*, 75 OR. L. REV. 117, 119 (1996).

122. *Id.*

123. Savage Sept. 27, *supra* note 3.

124. *Id.*

125. Savage Nov. 16, *supra* note 17; Martin, *supra* note 10, at 175.

126. Martin, *supra* note 10, at 176.

innovation of telecommunications technologies.[127] Landau points out that innovators would no longer "be able to have an idea, develop it, and go to the market; instead, early on, they would need to consult with the FBI. They would need lawyers and lobbyists—and time."[128] Such a requirement would definitely interfere with innovative processes, which in turn could threaten national security due to the importance of maintaining the United States' scientific and industrial strength.[129]

The threat to innovation could also cripple the position of American products within the global market. This was a fear of encryption makers in the late 1990s, which is renewed today in light of the CALEA proposal, as many believe that forcing regulations on U.S.-developed technology would drive the market for innovation overseas.[130]

E. International Impact

The expansion of CALEA would also have a significant international impact, both through software implementation by foreign governments and the impact on international communication and international commerce. The technologies developed to carry out the CALEA orders could be utilized by other governments in ways that remove or diminish the privacy of their citizens on the Internet. Even the Departments of Commerce and State have expressed fear[131] that such technologies would be "used by repressive regimes to hunt for political dissidents."[132]

Foreign corporations would also be impacted by the CALEA expansion as the government would require them to comply with the law through the services they provide to American consumers. Affected companies might include Research in Motion (the Canadian maker of BlackBerry devices) and others that have services based overseas.[133] Overseas-based services would have to change the design of their systems so that messages could be intercepted and unscrambled and would therefore "have to route communications through a server on United States soil where they could be wiretapped."[134]

The expansion of CALEA would therefore have significant international impact, which would not only encourage repressive actions by

---

127. *Id.*
128. Landau, *supra* note 5, at 428.
129. *Id.*
130. Savage Sept. 27, *supra* note 3; Martin, *supra* note 10, at 179.
131. Savage Nov. 16, *supra* note 17.
132. *Wiretapping and Other Eavesdropping Devices and Methods*, *supra* note 1.
133. Savage Sept. 27, *supra* note 3; Savage Nov. 16, *supra* note 17.
134. Savage Nov. 16, *supra* note 17.

foreign regimes but would also unfavorably constrain international companies and service providers to the requirements of the law.

VI. REASONS GIVEN FOR EXPANDING CALEA

Those opposed to CALEA have presented extensive arguments detailing the dangers of the proposal, to which the FBI and the Obama administration have, to some extent, countered to defend their position. The government argues that as the expansion of CALEA is within the scope of its current authority under wiretap law and that it does not create danger to the magnitude that its opponents allege; the CALEA expansion is, therefore, needed to serve the government interest in preventing and investigating crime.

A. Within Scope of Government Authority

In response to the arguments that the proposal of the Obama administration to expand CALEA is unwise and likely to cause an abundance of problems, the FBI argues that the proposal would not have detrimental consequences because it is not an expansion of law enforcement authority to wiretap. The CALEA provisions do not affect the legality of wiretaps nor the requirements imposed on law enforcement officials for obtaining wiretap orders. Valerie E. Caproni, General Counsel to the FBI, stated that the expansion would address lawfully authorized intercepts and that the FBI is promoting the expanded CALEA provisions to preserve the "ability to execute our existing authority in order to protect the public safety and national security."[135] The government argues these provisions are merely an attempt to keep up with criminal and terrorist activity in a world in which communication increasingly occurs online.[136]

B. Government Interest in Preventing and Investigating Crime

An important part of law enforcement is undeniably the ability to investigate and prevent crime through lawful use of wiretap and surveillance capabilities. As the world has transitioned to a significant portion of all communications occurring on the Internet, federal law enforcement and national security officials argue that their ability to wiretap is "'going dark' as people increasingly communicate online instead of by telephone."[137] The Internet has been increasingly used by criminals and terrorists for the very purpose of avoiding surveillance by law

135. Savage Sept. 27, *supra* note 3.
136. *See* Editorial, *supra* note 68.
137. Savage Sept. 27, *supra* note 3.

enforcement, and the inability of the FBI to wiretap adequately has led to some situations in which potentially preventable crimes occurred.

One example that has been widely reported in the media is that some of the September 11th hijackers may have used public computers in Florida and New Jersey to access the Internet and communicate with each other.[138] Two of the hijackers used a state college library in New Jersey to review and order airline tickets on the flight that crashed into the Pentagon.[139] Wisconsin Representative James Sensenbrenner, Jr., saying that it puts Americans' lives at risk, argued that such places should not be permitted to be sanctuaries for terrorists to operate.[140]

In 2010, an investigation into a drug cartel failed because the smugglers used peer-to-peer software that was tough to intercept, and, instead, the investigators had to install equipment in a suspect's office.[141] The delay "prevented the interception of pertinent communications."[142] In her statement to the House Judiciary's Subcommittee on Crime, Terrorism and Homeland Security on February 17, 2011, Valerie E. Caproni discussed two other situations that occurred recently, where the government was unable to gain more information on suspects because of the inability of the FBI to wiretap their communications.[143] One example was that the Drug Enforcement Agency, in an investigation of the leader of a criminal organization involved in cocaine smuggling, realized that the suspect was a former law enforcement officer who "went to great lengths to utilize communications services that lacked intercept solutions," and the government was unable to obtain enough information through other techniques.[144] Caproni's other example was a child prostitution case, in

---

138. Martin, *supra* note 10, at 153–54 (footnote omitted); *9/11 Hijackers Used Public Libraries*, WASH. TIMES, April 28, 2005, *available at* http://www.washingtontimes.com/news/2005/apr/28/20050428-115527-9817r/; Sue Anne Pressley & Justin Blum, *Hijackers May Have Accessed Computers at Public Libraries; Authorities Investigating Possible Internet Communications*, WASH. POST, Sept. 17, 2001, at A04, *available at* http://pqasb.pqarchiver.com/washingtonpost/access/80829842.html?FMT=ABS&FMTS=ABS:FT&date=Sep+17%2C+2001&author=Sue+Anne+Pressley+and+Justin+Blum&pub=The+Washington+Post&edition=&startpage=A.04&desc=Hijackers+May+Have+Accessed+Computers+at+Public+Libraries%3B+Authorities+Investigating+Possible+Internet+Communications.

139. *9/11 Hijackers Used Public Libraries*, *supra* note 138.

140. *Id.*

141. Savage Sept. 27, *supra* note 3.

142. *Id.*

143. *See Going Dark: Lawful Electronic Surveillance in the Face of New Technologies: Hearing Before the Subcomm. On Crime, Terrorism, and Homeland Sec. of the H. Comm. on the Judiciary*, 112th Cong. 2 (2011) (statement of Valerie Caproni, General Counsel, FBI), http://judiciary.house.gov/hearings/pdf/Caproni02172011.pdf [hereinafter *Hearing*].

144. *Hearing*, *supra* note 143, at 2.

which a social networking site used by the suspect did not have wiretap capabilities, and the FBI argued that although it was able to prosecute, the case was weaker and the resulting sentence was lighter than it may have been otherwise.[145] Due to the increasing communication over the Internet by criminals and terrorists, the government argues that the expansion of CALEA is necessary to maintain public safety and national security.

Although the government argues its surveillance capabilities are disappearing, in 2009, law enforcement agencies utilized a record 2,376 wiretaps, each yielding an average of 3,763 intercepted communications.[146] Privacy advocates argue that these numbers suggest that the FBI is "experiencing a boon in electronic surveillance" rather than being thwarted by technological barriers.[147]

C. Current Retrofit Services Delay Ability to Wiretap

The FBI and federal officials argue that the CALEA proposal should also move forward due to the problems that the government faces using old methods of wiretapping over the Internet. In many cases, if the FBI wants to wiretap a suspect who is using the Internet, it must retrofit a communications network, which can delay the process for months.[148] When a service is encrypted, sometimes even the provider cannot unscramble it, which prevents federal agents from obtaining communications at all.[149] Officials disagree with the allegation that installing access points will create weaknesses that would then be used by hackers to view the same information that the government is gathering. Instead, the government argues that building interception capability into service providers is less likely to "inadvertently create security holes than retrofitting it after receiving a wiretap order."[150]

In response to the accusation that the expansion of CALEA would be a serious threat to innovation, government officials point out that the same fear was prevalent when CALEA was first enacted in 1994 and that critics argued that the law would "impede cellphone innovation, but that technology continued to improve."[151] Government officials, therefore, argue that the CALEA expansion is necessary to maintain their ability to

---

145. *Id.*

146. *FBI Seeks New Mandates on Communications Technologies*, CTR. FOR DEMOCRACY & TECH. (Feb. 24, 2011), http://www.cdt.org/policy/fbi-seeks-new-mandates-communications-technologies.

147. *Id.*

148. Savage Sept. 27, *supra* note 3.

149. *Id.*

150. *Id.*

151. *Id.*

conduct law enforcement and maintain national security in the best interests of the American people.

VII. MORE INFORMATION REQUIRED TO BALANCE COMPETING INTERESTS ADEQUATELY

The Obama administration's proposal to expand CALEA to enable the FBI to require all communications services to be wiretap-capable has created debate over whether government interests would truly be met, and whether government interests outweigh the opposing concerns. As there are a number of competing interests on both sides of the debate, and significant factors indicate that the detrimental nature of a CALEA expansion would outweigh the government's interests, more information should be provided before any further steps are taken.

A. Competing Interests

The proposed legislation is representative of the strengthening relationship between the government and the private sector with regard to the Internet. The FBI cooperates extensively with networks as it is, and the proposals would advance this relationship further. This has created fear among some that the relationship will become a threat to the online environment.[152]

Other concerns regarding the expansion of CALEA include the fear that it will chill online speech that has a positive impact on society and that it will threaten valued American privacy.[153] Further reservations have been voiced regarding the negative impact CALEA would have on the aspects of Internet structure which contribute to its economic fruitfulness.[154] The design of the Internet would also be a problem for national security reasons as the software, which would be introduced for networks to comply with CALEA, could introduce vulnerabilities into the system that could be abused by hackers to access critical data. There are also misgivings about the software that would be created to wiretap the Internet because of the potential consequences it could have in the hands of repressive regimes and the harm it could cause to foreign corporations.[155]

The government argues that CALEA should be expanded because it is not an extension of current government authority to wiretap under the law

---

152. Birnhack & Elkin-Koren, *supra* note 28, at para. 3.

153. Horn, *supra* note 112, at 750 (quoting Frederick Schauer, *Fear, Risk and the First Amendment: Unraveling the 'Chilling Effect*,*'* 58 B.U. L. REV. 685, 693–700 (1978)).

154. Editorial, *supra* note 68.

155. *Wiretapping and Other Eavesdropping Devices and Methods*, *supra* note 1; Savage Nov. 16, *supra* note 17.

and it would advance significant state interests.[156] Emphasizing the importance of being able to wiretap in order to prevent and investigate crime, the FBI argues that there have been times that crimes have occurred when it could have been prevented had the capabilities to intercept Internet communications been available.[157] The FBI also argues that the potential for vulnerabilities to be exposed to hackers are even greater if the services have to be retrofitted rather than introduced through CALEA software.[158]

B. Lack of Information

In spite of these relevant government interests, the disparity between the arguments remains too large to justify the current expansion of CALEA. Along with the numerous critiques of the Obama administration's proposal to expand CALEA is the point that there is little public data about the frequency with which "court-approved surveillance is frustrated because of a service's technical design."[159] The ACLU argued in front of the House Judiciary Subcommittee on Crime, Terrorism and Homeland Security on February 17, 2011 that the expansion of the government's ability to wiretap the Internet is unnecessary because "[t]he number of wiretap orders the government seeks every year is a matter of public record and that record does not support this level of privacy invasion."[160] In the 2009 Wiretap Report, there were only thirty-two computer wiretap orders and only one encrypted communication order.[161] For the one encrypted communication order, law enforcement eventually gained access to the clear text of the communication.[162]

At the same hearing in front of the House Judiciary Subcommittee, the General Counsel of the FBI, Valerie E. Caproni, made updated statements about the intentions of the government with regard to the proposed expansion in the law.[163] Caproni announced that in the 2012 fiscal year, the government intends to establish a Domestic Communications Assistance Center ("DCAC") which would "leverage the research and development efforts of Federal, State, and local law enforcement with respect to electronic surveillance capabilities, facilitate the sharing of technology between law enforcement agencies, advance

156. Savage Sept. 27, *supra* note 3.
157. *Hearing*, *supra* note 143, at 2.
158. Savage Sept. 27, *supra* note 3.
159. *Id.*
160. Murphy & Calabrese, *supra* note 4, at 5.
161. *Id.*
162. *Id.*
163. *See Hearing*, *supra* note 143, at 7.

initiatives to implement solutions complying with CALEA, and seek to build more effective relations with the communications industry."[164]

Caproni also stated that the government "does not have a formal position . . . on whether any legislative changes are necessary," appearing to be possibly retreating from previous statements made by the administration.[165] Whether there is a formal position or not, the government has been moving toward a legislative change, and Caproni herself said that the Obama administration is looking forward to working with Congress to find a solution.[166] Documents obtained through a Freedom of Information Act request by the Electronic Frontier Foundation also demonstrate that "the FBI and Justice Department have been working on amendments to CALEA since 2006 and have been lobbying Congress and the White House to support it."[167]

The potential consequences of what could occur in the wake of a CALEA expansion, therefore, seem unjustified. Before enacting any new CALEA provisions into law, Congress should strongly consider whether the changes are truly necessary or whether the current capabilities of the FBI to wiretap Internet users are sufficient.[168] As discussed, there are competing interests that need to be taken into account, but since the FBI has not given substantial information about the reasons that these broad changes are needed, significantly more data should be gathered in order to best address these interests before CALEA is expanded.

C. Moving Forward

In order to balance the interests at hand more effectively, the creation of the DCAC, as discussed by Valerie Caproni, could gather further information about why exactly the change of CALEA is required for government interests to be met. This information should then be given to Congress and the American public, before further legislative action occurs, to ensure that additional Internet wiretapping capabilities for the government are truly necessary. The information gathered by the DCAC could be delivered in a method similar to the yearly Wiretap Report, providing transparency for the American public to track the extent to which their communications are being monitored. All that would be required on

---

164. *Id.*

165. *Id.*

166. *Id.*

167. Eric W. Dolan, *FBI Urges Congress to Expand Internet Wiretapping*, THE RAW STORY (Feb. 17, 2011), http://www.rawstory.com/rs/2011/02/17/fbi-urges-congress-to-expand-internet-wiretapping.

168. *See, e.g.*, Editorial, *supra* note 68.

such a report is the raw data, as it would be unwise to include specific examples that could lead suspects to realize that they are under government surveillance. The DCAC should work with the FBI to create such a report to demonstrate the extent to which government efforts to prevent and investigate crime have been foiled by the failure to wiretap Internet communications. Whether the government would have had the ability to get the information through other legitimate means when compiling the report should also be taken into account.

As the proposed DCAC is also suggested to "leverage existing research and development efforts of federal law enforcement,"[169] the DCAC could conceivably work to develop advanced technology that would avoid the current dangers from inserting access points into the existing Internet structure. If these proposed objectives are satisfied, the DCAC itself might assist in confronting some of the current dangers surrounding an expansion of CALEA. Landau and the Internet Engineering Task Force ("IETF"), an "international community of researchers who seek to provide standards to the evolution of the Internet's architecture," agree that the design of a "more secure Internet amenable to law enforcement purposes" could be plausible.[170] Their present concerns are focused on inserting access points in the Internet as it is presently structured and the "inherent security problems it would create."[171]

With systems as they currently exist and the information currently provided, it does not appear that the government could provide a strong enough argument for Internet wiretapping capabilities to outweigh the prevailing interests of the American public. The expansion of CALEA would partially infringe on the constitutionally provided First and Fourth Amendment freedoms and would create problems for industry development and national security. The government has a high burden of proof to demonstrate that such risks would be worth extending CALEA wiretapping to all Internet communications. The handful of examples provided by the government thus far should not be found by Congress to be worth justifying the expansion. The FBI and the Obama administration should, therefore, reconsider their proposal in light of the potential threats their actions could have on the security and well-being of the American public.

---

169. *U.S. Department of Justice FY 2012 Budget Request*, DEP'T OF JUSTICE, http://www.justice.gov/jmd/2012factsheets/docs/fy12-national-security.pdf.

170. Park, *supra* note 74, at 618–19. Landau in fact supported the funding for the DCAC when Caproni introduced it at the February 17, 2011 hearing. *FBI Seeks New Mandates on Communications Technologies*, *supra* note 146.

171. Park, *supra* note 74, at 619.

VIII. CONCLUSION

Although a formal proposal has yet to be introduced, the American public should be wary of the steps that the government is taking to extend wiretapping capabilities to all Internet communications. While the government argues that it has been losing the opportunity to obtain valuable information about suspects who violate the law due to their communication through the use of Facebook, Skype, and BlackBerry, there are noteworthy hazards which could arise through an expansion of CALEA. Threats to constitutional rights and national security are ultimately what our country faces if the Obama administration and the FBI are successful in their attempts to create Internet access points that could be manipulated by our enemies.

The looming fears surrounding the potential amendment of CALEA are substantively justified and demonstrate that there is much that needs to be addressed before Congress takes steps that potentially put our country in danger. The FBI should, therefore, utilize the soon-to-be created DCAC to gather more data to support the government's allegations that it is missing out on collecting critical information due to its inability to wiretap some Internet communications. Once this information is gathered, it is still likely that a realistic evaluation of competing interests will show that there is entirely too much at stake to allow the government to wiretap the Internet.