Tulsa Journal of Comparative and International Law

Volume 15 | Issue 2 Article 8

3-1-2008

Big Brother Hears You, but Can He Understand What He Hears - The Problematic Application of CALEA to VOIP Communications in the Age of Encryption

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

*Timothy Singleton**

> Because of advances in telecommunications networks, the introduction and deployment of new digitally-based technologies, services and features, law enforcement's ability to conduct court authorized surveillance is being threatened . . . the costs incurred to remove this threat to public safety and national security pale in comparison to the devastating economic impact, as well as the loss of life, if law enforcement's wiretapping efforts continue to be hampered by technological impediments.[1]
>
> -Louis J. Freeh, Former Director of the Federal Bureau of Investigation
>
> Whenever a telephone line is tapped, the privacy of the persons at both ends of the line is invaded, and all conversations between them upon any subject, and although proper, confidential, and privileged, may be overheard. . . As a means of espionage, writs of assistance and general warrants are but puny instruments of tyranny and oppression when compared with wire tapping.[2]
>
> -Justice Brandeis, regarding wiretapping as violative of the Fourth and Fifth amendments

---

* J.D. Candidate May 2010, University of Tulsa College of Law and Master of Science in Computer Science Candidate May 2010, University of Tulsa College of Engineering and Natural Sciences, Tulsa, Oklahoma. I would like to thank my wife, Kelly Singleton, for her understanding, patience, and encouragement. I would also like to thank Dr. John Hale and Nathan Singleton for their assistance on the technical aspects of this paper. Finally, I would like to thank the staff and Editorial Board of the *Tulsa Journal of Comparative & International Law* for their support, advice, and feedback in preparing this publication.

1. *Wiretapping Access: Hearing Before the Subcomm. on Telecomm. and Fin. of the H. Comm. on Energy and Commerce*, 103d Cong. 2, 4-5 (1994) (statement of Louis J. Freeh, Director, Federal Bureau of Investigation).

2. Olmstead v. United States, 277 U.S. 438, 475-76 (1928) (Brandeis, J., dissenting) (majority opinion held wiretapping did not violate the unreasonable search and seizure provision of the Fourth Amendment or the self-incrimination provision of the Fifth Amendment).

I. INTRODUCTION

Imagine agents from the Federal Bureau of Investigation (FBI) performing investigations on suspected technologically savvy terrorists. The terrorists use Voice over Internet Protocol (VoIP) technology, such as Skype or Vonage, to make telephone calls. The FBI agents install a wiretap through the telecommunications company and listen to the terrorist calls. With the help of this electronic surveillance the FBI is able to obtain information on terrorist locations, meetings, and plans. Using this information, the FBI is able to circumvent a terrorist attack. Now imagine the terrorists encrypting their VoIP calls. Because of encryption, instead of critical information, the FBI is left with a judicially approved wiretap that renders no evidence other than garbled trash.

Voice over Internet Protocol (VoIP) offers communication over the Internet similar to normal telephone calls,[3] and as VoIP usage grows, the threat of criminal and terrorist activity employing this technology substantially increases.[4] The technological advances in the form and function of telephony have begun to reflect the age of the current wiretap legislation in the United States.[5] The problems of effective wiretapping facing the government carry in their shadow issues of personal privacy.[6] The United Kingdom's approach differs substantially from that of the United States; however, examining some aspects of the British method may prove essential to a considered and effective refurbishment of United States law.

Even though the implementation of the Communications Assistance for Law Enforcement Act (CALEA)[7] to managed VoIP systems will afford law enforcement entities some wiretap capabilities, the law is not focused enough to adequately fulfill its proposed function and must be amended to reflect the fundamental differences in the technology used by modern telecommunications providers. This comment analyzes the potential privacy issues and the problems of packet switched networks, peer-to-peer communications, and encryption as

---

3. FCC, VOICE OVER INTERNET PROTOCOL: FREQUENTLY ASKED QUESTIONS, http://www.fcc.gov/voip/.

4. Declan McCullagh, *Feds: VoIP a Potential Haven for Terrorists*, ZDNET NEWS, Jun. 16, 2004 http://news.zdnet.com/2100-1009-5236233.html.

5. *See* Jason Hill, *The Storm Ahead: How CALEA will turn VoIP on its Head* 1 (Kennesaw, Ga., Sept. 22-23, 2006) (Proceedings of the 2006 Information Security Curriculum Development Conference) (copy of paper on file with the *Tulsa Journal of Comparative and International Law*), *available at* http://delivery.acm.org/10.1145/1240000/1231079/p147-hill.pdf?key1=1231079&key2=0465707021&coll=GUIDE&dl=GUIDE&CFID=22450962&CFTOKEN=71691155.

6. *See* ELECTRONIC FRONTIER FOUNDATION, CALEA: THE PERILS OF WIRETAPPING THE INTERNET, http://www.eff.org/issues/calea (last visited Apr. 5, 2008).

7. Communications Assistance for Law Enforcement Act, 47 U.S.C. §§ 1001-10 (2006).

they apply to government wiretapping in the era of VoIP communications. Section II offers an overview of the nature of telephone and Internet communications. Section III provides a discussion of the basics of encryption and its application in VoIP. Section IV addresses a brief history of wiretapping, wiretap legislation in the United States, United Kingdom, and Europe, and the Fourth Amendment issues associated with wiretapping. Section V argues the problems facing CALEA's implementation, including tracking communication information across packet switched networks, the difficulty of tracking peer-to-peer communications, and timely deciphering encrypted data streams. Section VI compares and contrasts the methods of wiretapping in the United States and the United Kingdom and analyzes the need for careful wiretapping legislation. Section VII discusses suggested solutions to the balance of privacy and security. Section VIII concludes by proposing that CALEA, as applied to VoIP communications, will cause more problems with implementation and privacy concerns than it will solve, and therefore should not be applied to VoIP without carefully considered changes to its implementation.

II. BACKGROUND ON THE PUBLIC SWITCH TELEPHONE NETWORK AND VOICE OVER INTERNET PROTOCOL

A. The Public Switch Telephone Network Structure

The Public Switch Telephone Network (PSTN) is the network through which all conventional telephone calls are routed.[8] The PSTN and VoIP have different architectures which lead to increased difficulty in tapping the varying forms of VoIP communication.[9] To understand the differences between wiretapping traditional wireline and IP communications, it is necessary to introduce the differences between their architectures. The telephone network is based on the creation of physical or logical circuits between the two parties of a conversation.[10] A circuit switched network, like the PSTN, requires that the destination and source, the caller and the person being called, be connected by a circuit before communication can take place.[11] The circuit between the two parties to the call functions as a direct cable between the parties without

8. LILLIAN GOLENIEWSKI, TELECOMMUNICATIONS ESSENTIALS: THE COMPLETE GLOBAL SOURCE 103 (Kitty Wilson Jarrett ed., Addison-Wesley 2d ed. 2007) (2006).

9. STEVEN BELLOVIN ET AL., SECURITY IMPLICATIONS OF APPLYING THE COMMUNICATIONS ASSISTANCE TO LAW ENFORCEMENT ACT TO VOICE OVER IP, INFORMATION TECHNOLOGY ASSOCIATION OF AMERICA 5 (2006), http://www.itaa.org/isec/docs/CALEAVOIPreport.pdf.

10. *See* GOLENIEWSKI, *supra* note 8, at 100.

11. OLIVER C. IBE, CONVERGED NETWORK ARCHITECTURES: DELIVERING VOICE OVER IP, ATM, AND FRAME RELAY 2 (Margaret Eldridge ed., John Wiley & Sons, Inc. 2002).

interruption.[12] Once established, the circuit provides negligible delay and a high quality of service.[13] The delay experienced in telephone traffic is the delay in time it takes the signal to travel from one party to the other and is not noticeable to most subscribers.[14] Individual subscribers connect to the telephone network via their local loop, the last length of cable between the actual telephone and the larger network lines.[15] This loop connects to the switching nodes that route traffic through the network.[16] Switching nodes create the circuit which stretches from the local loop of the caller across several switching nodes, and finally end at the local loop of the call recipient.[17]

Early wiretaps were often connected at the local loop, directly to the copper wire between the dwelling or business and the main telephone line.[18] This allowed the listener to catch all the information passing through the loop, but no information that stopped or was redirected at or before the switch.[19] Because forwarded calls are redirected at the switch, never passing through the loop, a wiretap could not access a forwarded call.[20] When call forwarding is applied, for instance to a tapped phone line, the calls are transferred to another designated number.[21] Call forwarding applied to a tapped phone circumvents the wiretap entirely and allows for conversations free from government eavesdropping.[22] By the early 1990s, the leaps in telecommunications technology, such as fiber optic cables, wireless connections, and digital stored program control switches, made line wiretapping an inefficient way to conduct court-ordered wiretapping since it depended almost entirely on antiquated analog switching and copper wires to function properly.[23]

---

12. *Id.*

13. *See id.*; *see also* GOLENIEWSKI, *supra* note 8, at 100.

14. *See* GOLENIEWSKI, *supra* note 8, at 89.

15. IBE, *supra* note 8, at 14 ("The access network between a subscriber's telephone and the [central office] is called the local loop (or the last mile). . . . Wireless local loop, which uses radio links rather than physical wire, is becoming increasingly available.").

16. GOLENIEWSKI, *supra* note 8, at 111.

17. *See id.* at 7-8.

18. BELLOVIN ET AL., *supra* note 9, at 5.

19. *See id.*

20. *Id.*

21. *See* AT&T, User Guide Call Forwarding, http://www01.sbc.com/Products_Services/Residential/1,409—5-3-0,00.html (last visited Apr. 5, 2008).

22. BELLOVIN ET AL., *supra* note 9, at 5.

23. *See Wiretapping Access: Hearing Before the Subcomm. on Telecomm. and Fin. of the H. Comm. on Energy and Commerce*, 103d Cong. (1994) (statement of A. Richard Metzger, Jr., Deputy Chief Common Carrier Bureau, Federal Communications Commission) [hereinafter Metzger].

B. Voice Over Internet Protocol Structure

VoIP is a large and growing market for telecommunications.[24] In the third quarter of 2007, Vonage boasted 2.446 million subscriber lines.[25] By the end of September 2005, Skype claimed more than 100 million registered users.[26] One market analysis group estimated that in 2006 alone, VoIP services saw an increase of thirty-four million subscribers worldwide.[27] As director of the FBI, Louis J. Freeh stated, currently "[t]he nation's telecommunications networks are routinely used in the commission of serious criminal activities, including terrorism, organized crime, drug trafficking, violent crime, espionage, fraud, and other white collar crime."[28] As residential, business, and government use of VoIP grows and becomes more common, so will the need for law enforcement wiretaps of those communications.[29]

IP telephony utilizes a packet switching network[30] and comes in several different varieties.[31] Packet switching breaks up the call information into packets which are sent over the network.[32] These packets can be different sizes, composed of different numbers of bits, and contain varying amounts of navigational information.[33] The navigational information is used by network nodes to route the packet to the proper destination.[34] Unlike circuit switch networks, packet switching does not require the circuit between the source and destination to be established before the beginning of communication.[35] The navigational information in the header determines where the packet is going and

---

24. *See generally* Vonage Company Profile, Third Quarter 2007, Vonage, http://files.shareholder.com/downloads/VAGE/189723027x0x56424/ad50fa02-58fb-4dc5-abfc-5bd1100ce9be/FactSheet.pdf (last visited Apr. 5, 2008).

25. *Id.*

26. Skype Hits 100M Subscriber Mark, http://www.news.com/8301-10784_3-6066399-7.html (Apr. 28, 2006, 23:05 PDT)[hereinafter Skype Hits 100M].

27. Jan Harris, *VoIP Attracts 34 Million New Subscribers*, VOIP NEWS, July 9, 2007, http://www.voip-news.co.uk/2007/07/09/voip-attracts-34-million-new-subscribers/.

28. Declaration of FBI Director Louis J. Freeh at 2-3, Communications Assistance for Law Enforcement Act, 14 F.C.C.R. 16794, C.C. Docket No. 97-213 (Third Report and Order)(1999), *available at* http://www.askcalea.net/lef/docs/990127-f.pdf [hereinafter Freeh].

29. *Id.*

30. *See* GOLENIEWSKI, *supra* note 3, at 92-93.

31. *See generally* Patrick Barnard, *Internet Engineers Reveal Difficulties in Applying CALEA to VoIP*, TECHNOLOGY MARKETING COMPANY NET.COM, June 21, 2006, http://ipcommunications.tmcnet.com/hot-topics/ims/articles/1617-internet-engineers-reveal-difficulties-applying-calea-voip.htm (explaining that the installation of any wiretapping features will be difficult given the different system architectures offered by VoIP service providers).

32. IBE, *supra* note 14, at 2.

33. GOLENIEWSKI, *supra* note 8, at 93.

34. *Id.*

35. IBE, *supra* note 14, at 2.

in what order it should be reconstructed.[36] The packet switch network can be either connectionless or connection-oriented.[37] Packets in a connectionless environment may all take different routes from source to destination.[38] A connection-oriented packet switch network acts similar to the circuit switch architecture.[39] Because of this difference between connectionless and connection-oriented packet switching, CALEA cannot operate in the same way on all VoIP services as it does on the PSTN.[40] CALEA wiretaps work by requiring that telecommunication providers ensure their switches and other equipment have features and services that aid law enforcement in wiretapping.[41] This type of wiretapping presumes and requires that information be sent over a specific switch.[42] Because the Internet does not have to send all packets from a VoIP communication over one switch, the standard wiretap may be ineffective at obtaining the information desired.[43]

In addition to the differences between packet switch and circuit switch communications; VoIP comes in several different types.[44] For the purposes of this comment, the four types of VoIP communication discussed will involve the relation of the communication to the PSTN, which will allow further discussion of wiretapping capabilities. The first type of IP telephony service is computer-to-computer.[45] In the computer-to-computer service, both the source and destination users use the same VoIP service application.[46] Computer-to-computer communications do not employ the PSTN.[47] The second type of

---

36. *See* GOLENIEWSKI, *supra* note 8, at 93.

37. *Id.* at 95.

38. *See id.* at 96.

39. *Id.* at 97 ("In a connection-oriented packet-switched network, only one call request packet contains the source and destination address . . . . The call request packet establishes the virtual circuit.").

40. *See* BELLOVIN ET AL., *supra* note 9, at 8.

41. *See* Metzger, *supra* note 23.

42. *See* WHITFIELD DIFFIE & SUSAN LANDAU, PRIVACY ON THE LINE: THE POLITICS OF WIRETAPPING AND ENCRYPTION 220-21 (MIT Press 2007) (1998).

43. *See id.*; *see also* Metzger, *supra* note 23.

44. Barnard, *supra* note 31.

45. Types of VoIP Configurations You Might See, VoIP FAQ, http://www.voipfaq.net/types+of+voip.php, [hereinafter VoipFAQ] (last visited Apr. 6, 2008); *see also* Robert Valdes, *How VoIP Works*, HOWSTUFFWORKS.COM, http://communication.howstuffworks.com/ip-telephony.htm (last visited Apr.6, 2008).

46. *See* OFCOM, REGULATION OF VOIP SERVICES: ACCESS TO THE EMERGENCY SERVICES 7(2007), http://www.ofcom.org.uk/consult/condocs/voip/voip.pdf [hereinafter OFCOM];OFCOM is "the independent regulator of television, radio, telecommunications and wireless communications services in the [United Kingdom]." *Id.* at 1.

47. *See id.* at 7.

service is computer-to-phone.[48] Computer-to-phone communications transfer the call from the originating computer to a PSTN exchange and then route it as a normal telephone call.[49] The third type of service is phone-to-computer.[50] Phone-to-computer communications use the same style of contact as computer to phone, but in reverse.[51] The computer user receives calls from a telephone network exchange which is transferred to the VoIP service provider from the PSTN exchange.[52] The fourth and final type of communication involves IP phones.[53] These telephones are specialized, connecting directly to a router,[54] but are capable of being assigned an ordinary geographic telephone number or a VoIP number.[55] IP phones have the capability of both the computer-to-computer and computer-to-phone communications.[56]

Different types of VoIP communication mean different problems with wiretapping.[57] When an interception is attempted against an IP communication at a fixed location with a fixed number (or Internet address) connecting directly to a large Internet Service Provider (ISP) or connecting to the PSTN, the wiretap works much the same way as a tap against the telephone line.[58] Wiretaps against IP phones and desktop computer based VoIP services have at least the potential to work in the same method as those on the regular telephone network.[59] However, VoIP communications do not require fixed locations.[60] These calls simply require an Internet connection.[61] Internet connections do not always lead to fixed IP addresses.[62] In fact, if the service on the laptop or

---

48. VoipFAQ, *supra* note 45.

49. *Id.*; *see also* OFCOM, *supra* note 46, at 7.

50. OFCOM, *supra* note 46, at 7.

51. *Id.*

52. *Id.*; *see also* VoipFAQ, *supra* note 45 (noting that computer-to-phone service also works in much the same manner as computer-to-computer).

53. Valdes, *supra* note 45.

54. *Id.*

55. OFCOM, *supra* note 46, at 7-8.

56. VoipFAQ, *supra* note 45.

57. BELLOVIN ET AL., *supra* note 9, at 2.

58. *Id.*; *see also* OFCOM, *supra* note 46, at 8.

59. *See* BELLOVIN ET AL, *supra* note 9, at 2.

60. OFCOM, *supra* note 46, at 8.

61. *Id.* ("Also, a VoIP service can be for use on the move using wireless broadband (WiMAX or Wi-Fi). VoIP can, therefore, be a mobile service, sometimes known as Voice over Wireless (VoWLAN).").

62. More About Networking: What are Static IP, Dynamic IP, and Network Address Translation (NAT)?, USROBOTICS, http://www.usr.com/education/net9.asp [hereinafter USROBOTICS]

([N]ot every machine on the Internet can have a static IP address. In the current IP protocol, there are a limited number of numbered IP addresses, and they need to be conserved. Chances are

desktop computer is connected to the ISP through a router or firewall, a different IP address may be assigned each time the computer requests a new IP address.[63] Similarly, laptops and VoIP capable mobile devices can connect to the Internet through wireless access points around the world.[64] Each time they connect to a different access point, the IP address usually changes.[65]

Aside from IP address difficulties, the larger problem is that of computer-to-computer, or peer-to-peer, connections.[66] Peer-to-peer VoIP communications have been thought to be secure from tracking.[67] If the IP address is known, however, a watermark may be embedded into the communication traffic and can be traced to the destination IP address; meaning that encrypted and anonymous peer-to-peer communications *can* be tracked.[68] Certain peer-to-peer service providers encrypt their communications to allow a modicum of privacy for their users.[69] There are, however, multiple ways to track anonymous and encrypted VoIP traffic.[70] One example of tracking occurred recently when a criminal was traced to Sri Lanka after placing a one minute VoIP call.[71] Though tracking an anonymous and encrypted peer-to-peer communication can be useful in locating criminals, it does not meet the standard of wiretapping envisioned by CALEA.[72] Under those requirements, the interception of calls must include call-identifying information and call content.[73] The call content requirement is a particular

---

(unless you request it or you purchase more costly "Business" high-speed internet access) you use a Dynamic IP address.) (last visited Apr. 6, 2008).

63. BELLOVIN ET AL, *supra* note 4, at 16.; *see also* USROBOTICS, *supra* note 55; *see also* GOLENIEWSKI, *supra* note 3, at 275 ("In dynamic [Network Address Translation], a private IP address is mapped to a public IP address drawn from a pool of registered public IP addresses. By keeping the internal configuration of the private network hidden, dynamic [Network Address Translation] helps conceal the network from outside users.").

64. *See* OFCOM, *supra* note 46, at 8.

65. *See* BELLOVIN ET AL., *supra* note 9, at 16.

66. *See id.* at 3, 13-14.

67. *See* Xinyuan Wang et al., *Tracking Anonymous Peer-to-Peer VoIP Calls on the Internet*, (Alexandria, VA, Nov. 7-11,2005) (Proceedings of 12th ACM Conference on Computer Communications Security) (copy of paper on file with the *Tulsa Journal of Comparative & International Law*)
http://ise.gmu.edu/%7exwangc/Publications/CCS05-VoIPTracking.pdf.

68. *Id.*

69. *Id.* at 2.

70. *See id.*

71. Eric Bangeman, *Fugitive Exec Nabbed After Skype Call*, ARS TECHNICA, Aug. 24, 2006, http://arstechnica.com/news.ars/post/20060824-7582.html ("Alexander was traced to the Sri Lankan capital of Colombo after he placed a one-minute call using Skype.").

72. 47 U.S.C. §§ 1001-10 (2006); *see also* 18 U.S.C. § 2510 (2006).

73. 47 U.S.C. § 1002 (a)(1-2).

problem for law enforcement wiretaps on VoIP communications and is the focus of this paper.

III. BACKGROUND OF ENCRYPTION AND ITS APPLICATION TO VOIP

A. The Basics of Encryption

Given infinite time and resources, all encryption ciphers can be broken. Encryption is the process of disguising the substance of a message so that it cannot be read by an undesired party.[74] Decryption is the process of turning that disguised message back into a readable form.[75] The process of encryption and decryption requires four basic elements.[76] The first of these elements is the message to be encrypted, which is normally referred to as the plaintext.[77] The second is a secret key which both parties know.[78] The third and fourth elements are an encryption algorithm and a decryption function, respectively.[79] Using the encryption algorithm on the plaintext creates what is known as ciphertext.[80] If the encryption is done properly, the ciphertext will be readable only after it has been decoded, which requires the use of the key.[81]

Encryption and decryption require the exchange of secret information, the key, before messages can be encoded and decoded.[82] Keys are generated from a mathematical algorithm which is designed to produce a new, unique key each time the algorithm is used.[83] One of the most important principles in cryptography is that of Kerckhoff.[84] First published in 1883, Auguste Kerckhoff indicated that a system must not require secrecy,[85] and the security of the system

---

74. BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY, PROTOCOLS, ALGORITHMS, AND SOURCE CODE IN C 1 (Phil Sutherland ed., 2d ed. John Wiley & Sons 1996).

75. *Id.*

76. *See* NIELS FERGUSON & BRUCE SCHNEIER, PRACTICAL CRYPTOGRAPHY 22 (Carol A. Long ed., Johns Wiley & Sons 2003).

77. *Id.*

78. *Id.*

79. *Id.*

80. SCHNEIER, *supra* note 74, at 1.

81. FERGUSON & SCHNEIER, *supra* note 76, at 22.

82. Historical, Frequently Asked Questions, Chapter 1 Introduction, 1.2 What is Cryptography?, RSA Laboratories, http://www.rsa.com/rsalabs/node.asp?id=2157 (last visited Apr. 6, 2008).

83. *See* SCHNEIER, *supra* note 74, at 4.

84. FERGUSON & SCHNEIER, *supra* note 76, at 23.

85. Auguste Kerckhoff, *La Cryptographie Militaire*, IX JOURNAL DES SCIENCES MILITAIRES 5 (1883) (translation by Fabien Petitcolas, *available at* http://www.petitcolas.net/fabien/kerckhoffs/ (last visited Apr. 6, 2008)).

should be based solely on the security of the key.[86] Encryption algorithms that require keeping secret the way the algorithm works are called restricted algorithms.[87] These systems are inadequate under current standards because groups constantly change members.[88] Each time a member leaves the group, the remaining members must change their algorithm which requires development time and is expensive for the users.[89] Because of the time and cost constraints of constantly changing the algorithm, keys were developed which could easily be changed without affecting the algorithm.[90] The result was an inexpensive and effective way to maintain message encryption in an ever-changing environment.[91] Even if an eavesdropper knows the algorithm used to encrypt and decrypt the message, if the key is secret, the message remains unreadable.[92] The key for encryption and decryption functions much the same way as a key in a lock.[93] An encryption key or decryption key either locks or unlocks the message so that it may be read or disguised.[94]

There are two types of key based encryption/decryption algorithms.[95] The first is secret-key cryptography,[96] also called a symmetric algorithm.[97] These systems use an encryption key that can be used to calculate the decryption key, and vice versa.[98] Often, the same key is used for encryption and decryption.[99] Therefore, symmetric algorithms inseparably link the two functions,[100] and have historically been the standard in cryptography.[101] In these systems, the secrecy

---

86. FERGUSON & SCHNEIER, *supra* note 76, at 23.

87. SCHNEIER, *supra* note 74, at 3.

88. *Id.* (An example of this would include any group of individuals who decide that they wish to restrict access to their communications. When a member of the group leaves, in order to maintain security, the other members must change their restricted algorithms. This can cost the group valuable time, resources, and funds to create a new restricted algorithm. If this group happens to be a service provider, the cost is likely passed on to the end users.).

89. *See id.*; *see also* DIFFIE & LANDAU, *supra* note 42, at 13.

90. SCHNEIER, *supra* note 74, at 3.

91. *Id.*; *see also* DIFFIE & LANDAU, *supra* note 42, at 13.

92. SCHNEIER, *supra* note 74, at 3.

93. DIFFIE & LANDAU, *supra* note 42, at 13.

94. *Id.*

95. Historical, Frequently Asked Questions, Chapter 1 Introduction, 1.3, What are Some of the More Popular Techniques in Cryptography?, RSA Laboratories, http://www.rsa.com/rsalabs/node.asp?id=2158, [hereinafter RSA FAQ] (last visited Apr. 6, 2008).

96. *Id.*

97. SCHNEIER, *supra* note 74, at 4.

98. *Id.*

99. *Id.*

100. *See* DIFFIE & LANDAU, *supra* note 42, at 38.

101. *See* IAN CURRY, AN INTRODUCTION TO CRYPTOGRAPHY AND DIGITAL SIGNATURES 3 (2001), *available at* http://www.entrust.com/resources/pdf/cryptointro.pdf.

of the key is paramount because of its dual role.[102] Today, probably the most popular and widely used secret key system is the Data Encryption Standard (DES).[103]

In the past twenty years, the second form of encryption/decryption algorithm, called an asymmetric algorithm or public-key system, has dominated the course of cryptography.[104] This key system differs fundamentally from the symmetric algorithm.[105] The asymmetric algorithm uses a public key and a private key to encrypt and decrypt messages.[106] In public key systems, the private key can be used to either encrypt or decrypt a message.[107] If the private key is used to decrypt the message, the public key is used to encrypt it.[108] If the private key is used to encrypt the message, the public key will necessarily be used to decrypt it.[109] Despite the inverse nature of the keys in a public key system, it is computationally infeasible to discover one key given access to the other.[110] Though a public key system makes the issue of key secrecy simpler, it has two drawbacks.[111] The first is that public key systems are less efficient than symmetric key systems, by several orders of magnitude.[112] The second problem is that public key systems require some verification process to ensure the public key is used by the proper person.[113] Often, practical systems use a combination of symmetrical and public key encryption methods to secure communications.[114] Perhaps the most common version of public key encryption is Rivest, Shamir, and Adleman (RSA).[115]

Three of the most common encryption types are DES, RSA, and the Advanced Encryption Standard (AES).[116] AES is the new U.S. government

---

102. SCHNEIER, *supra* note 74, at 4.

103. RSA FAQ, *supra* note 82.

104. DIFFIE & LANDAU, *supra* note 42, at 38.

105. *See* FERGUSON & SCHNEIER, *supra* note 76, at 26.

106. *See* RSA FAQ, *supra* note 82.

107. DIFFIE & LANDAU, *supra* note 42, at 39.

108. *Id.*

109. *Id.*

110. *Id.*

111. *See* FERGUSON & SCHNEIER, *supra* note 76, at 28; DIFFIE & LANDAU, *supra* note 36, at 39.

112. FERGUSON & SCHNEIER, *supra* note 76, at 28.

113. DIFFIE & LANDAU, *supra* note 42, at 39; *see also* FERGUSON & SCHNEIER, *supra* note 76, at 29 (stating the job of the key management facility, or certification authority, who receives public keys from a subscriber and then attaches a digital signature that verifies that the certification authority identified the specific party as the owner of that public key).

114. FERGUSON & SCHNEIER, *supra* note 76, at 28.

115. RSA FAQ, *supra* note 82.

116. *See id*; VOIPREVIEW.ORG, VOIP SECURITY, http://voipreview.org/news.details.aspx?nid=7 (last visited Apr. 7, 2008).

encryption standard.[117] AES and DES have different structures.[118] DES can only be scaled to a 128-bit encryption by using three DES encryptions in sequence.[119] AES can easily be scaled up to 256-bit encryption, which is far beyond the current standard, and makes the time required to break the cipher exponentially longer.[120] RSA can be scaled up to 2048-bits for extremely valuable keys.[121] Though the above represent several common ciphers, there are myriad other encryption methods of varying degrees of strength and effectiveness.[122]

B. Encryption Options for VoIP

Currently, there are several ways in which VoIP communications may be encrypted.[123] Because these communications are broken into data packets, it is feasible to use common encryption methods already in use for online communications in text format.[124] For instance, Skype, a popular VoIP provider that functions by peer-to-peer connections, employs AES encryption which is used by U.S. government organizations to protect sensitive information.[125] Though AES can use as low as 128-bit encryption, Skype boasts a 256-bit encryption, which provides the possibility of 2^{256} unique keys.[126] Vonage, another popular version of IP phone, uses Session Initiation Protocol (SIP) instead of peer-to-peer technology.[127] Though Vonage does not currently employ encryption,[128] SIP phones have standardized security and encryption

---

117. FERGUSON & SCHNEIER, *supra* note 76, at 55.

118. *See id.* at 55-56.

119. *Id.* at 51.

120. *See id*; *see also* SCHNEIER, *supra* note 74, at 9.

121. *See* Frequently Asked Questions, Chapter 3 Techniques in Cryptography, 3.1.5 How Large a Key Should be Used in the RSA Cryptosystem?, RSA Laboratories, http://www.rsa.com/rsalabs/node.asp?id=2218 (last visited Apr. 7, 2008).

122. *See* FERGUSON & SCHNEIER, *supra* note 69, at 51-62.

123. *See* How to: Encrypt Your VoIP, VoIPNow.com, http://www.voipnow.org/2007/04/how_to_encrypt_.html (last visited Apr. 7, 2008).

124. *Id.*

125. TOM BERSON, SKYPE SECURITY EVALUATION 1-3 (Skype 2005), *available at* http://www.skype.com/security/files/2005-031%20security%20evaluation.pdf [hereinafter BERSON]; NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, INFORMATION TECHNOLOGY LABORATORY, ANNOUNCING THE ADVANCED ENCRYPTION STANDARD FEDERAL INFORMATION PROCESSING STANDARDS 1 (2001), *available at* http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf [hereinafter FIPS].

126. FIPS, *supra* note 125, at 1; BERSON, *supra* 124, at 3.

127. Tracy V. Wilson, *Skype v. Vonage*, HOWSTUFFWORKS.COM, http://electronics.howstuffworks.com/skype-vonage3.htm (last visited Apr.6, 2008).

128. *Id.*

capabilities.[129] This VoIP type can employ various types of encryption to protect the content of calls.[130] These communications can take advantage of a Virtual Private Network (VPN) client, which creates a secure channel between the source and destination of a call.[131] If VPN clients and Internet Protocol Security (IPsec)[132] do not afford the desired quality of service for a communication, the user can employ Secured Socket Layer (SSL)[133] technology, which is usually used to encrypt credit card purchases over the Internet.[134] VoIP can also use the strong encryption of a Secure Real-time Transport Protocol (SRTP),[135] which is already employed by a number of VoIP providers.[136] Technologically savvy individual users can also employ AES, DES, or RSA encryptions using either a self-constructed communication program or one already in place.[137] Because of the differences between these security protocols, a government organization seeking to break the encryption would first have to discover which type it is, and then plan an attack suited for that protocol.[138]

---

129. *See* Cisco, Overview of SIP Security 1-4 (Cisco 2008), *available at* http://www.cisco.com/en/US/docs/ios/12_3/vvf_c/cisco_ios_sip_security_application_guide/sipsecov.pdf.(last visited Apr. 8, 2008).

130. *See id.*; *see also* ALAN B. JOHNSTON, SIP: UNDERSTANDING THE SESSION INITIATION PROTOCOL 59-60 (2d ed. Artech House, Inc. 2004).

131. *See* Anthony Plewes, *The Dos and Don'ts of VoIP Security*, SILICON.COM, Apr. 4, 2007, http://www.silicon.com/research/specialreports/voipsecurity/0,3800013656,39166658,00.htm; *see also* D. RICHARD KUHN ET AL., NAT'L INST. OF STANDARDS AND TECH., SECURITY CONSIDERATIONS FOR VOICE OVER IP SYSTEMS 65-66 (U.S. Dept of Commerce 2005), *available at* http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58-final.pdf

132. Internet Protocol Security is a framework of protocols used to secure communications on the network or packet processing layer. SearchSecurity.com Definitions, http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci214037,00.html (last visited Apr. 6, 2008).

133. Secure Sockets Layer (SSL): How It Works, Verisign.com, http://www.verisign.com/ssl/ssl-information-center/how-ssl-security-works/ (explaining that Secure Socket Layer technology uses asymmetric or public key encryption to create "a secure session that guarantees message privacy and message integrity.")(last visited Apr. 6, 2008).

134. Plewes, *supra* note 131.

135. What is SRTP?, Whatis.com, http://whatis.techtarget.com/definition/0,,sid9_gci1233810,00.html (indicating that Secure Real-time Transport Protocol technology uses encryption and authentication to minimize the potential for certain attacks on a communication.)(last visited Apr. 6, 2008).

136. Plewes, *supra* note 131.

137. *See* KUHN ET AL., *supra* note 131, at 70.

138. *See generally* FERGUSON & SCHNEIER, *supra* note 76, at 55-58 (explaining that because of the complex structures of each protocol, the chances of an attack are low.)

IV. HISTORY OF WIRETAPPING

A. A Brief History of Wiretapping in the United States

To understand the impact of CALEA on wiretapping, it is necessary to cover the history of wiretapping in the United States. Although some believe wiretapping is an evil attempt to limit individual privacy,[139] it is more accurately an investigative tool with a secretive nature that invokes suspicion and a potential for abuse.[140] Wiretapping did not start with the telephone.[141] Civil War generals used telegraph wiretappers,[142] as did stockbrokers in the 1860s.[143] In the early 1890s, New York City police were the first to tap telephone lines for investigations.[144] Early wiretaps consisted of connections made to the wires running to telephone or telegraph poles, but evolved into the transmission of the tapped signal via an alternate line to a convenient and secure location for recording and monitoring.[145]

Before 1968, an agent assigned to tap a phone line only needed the help of the telephone company in determining the cable and pair numbers to make a tap on a particular line against a specific person.[146] The cooperation of telephone companies in court-ordered wiretaps was optional[147] until 1970, when the law was amended to provide that when requested, an order could contain directions to a carrier or other persons to provide assistance and information in the execution of the wiretap.[148] It was not until 1994 that legislation was created to require wiretapping capabilities to be built into the telephone system.[149] As wiretapping has become more sophisticated, its use has also increased.[150] This

---

139. *See Threats to Privacy*, PRIVACY INTERNATIONAL, Dec. 11, 2004, http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-82586#_Toc458240161.

140. DIFFIE & LANDAU, *supra* note 42, at 175.

141. *Id.* at 177.

142. *Id.*

143. *Id.* (citing SAMUEL DASH ET AL., THE EAVESDROPPERS 23 (Da Capo Press 1971) (1959).

144. DIFFIE & LANDAU, *supra* note 42, at 175 (citing DASH ET AL., *supra* note 142, at 35).

145. BELLOVIN ET AL., *supra* note 9, at 5.

146. EDITH J. LAPIDUS, EAVESDROPPING ON TRIAL 124 (Hayden Book Co. 1974) (explaining that "[l]aw enforcement agents need[ed] to know the cable and pair numbers in order to effectuate a tap on a particular telephone line – the *cable* in which the suspect's telephone line is located and the particular *pair* in the cable.").

147. *Id.* at 123.

148. *Id.*

149. Communications Assistance for Law Enforcement Act § 102, 47 U.S.C. § 1002(a)(1-3) (2006)

150. *See* ADMIN. OFFICE OF THE U.S. COURTS, 2006 WIRETAP REPORT 39 tbl. 9 (2006), *available at* http://www.uscourts.gov/wiretap06/Table92006.pdf [hereinafter WIRETAP REPORT].

growth can be seen from J. Edgar Hoover's denial of its usefulness until 1957,[151] to a total of 1839 intercept orders issued by judges over the course of the 2006 calendar year.[152]

B. Wiretap Legislation in the United States Before and up to CALEA

Under CALEA and earlier statutes, a wiretap must be performed in a way that minimizes interception of conversations that are not authorized by a warrant.[153] The Omnibus Crime Control and Safe Streets Act of 1968 created the first comprehensive framework for electronic surveillance in criminal investigations.[154] That framework allowed limited interception of oral and wire communications to be performed "(i) only when other investigative techniques have failed, reasonably appear unlikely to succeed, or are too dangerous to attempt, (ii) only for the investigation of serious, statutorily-specified felony offenses, and (iii) only for the interception of criminal communications."[155] CALEA built upon the Omnibus Crime Control and Safe Streets Act not by repeating the elements of the statute, but by requiring telecommunications providers to implement wiretap capabilities in their systems.[156] The substantive provisions of the later Act originally applied only to telecommunications carriers, which included little more than telephone companies.[157] This changed in June of 2006 with a decision from the United States Court of Appeals for the District of Columbia Circuit.[158] In *American Council on Education v. FCC*, the court ruled in a two-to-one decision that VoIP providers counted as telecommunications carriers and were subject to the wiretap capability provisions.[159]

CALEA requires telecommunications carriers to meet assistance capability requirements.[160] Instead of design specifications, it compels carriers to ensure

---

151. LAPIDUS, *supra* note 146, at 67 ("Until 1957 [Hoover] denied that organized crime existed and denounced wiretapping as a lazy man's tool and an obstacle" to the creation of sound investigative techniques.).

152. WIRETAP REPORT, *supra* note 150, at 15 tbl. 2.

153. CLIFFORD S. FISHMAN & ANNE T. MCKENNA, WIRETAPPING AND EAVESDROPPING §8:34, at 8-59 (2d ed. West 2004) (1978); *see also* 47 U.S.C. § 1002 (a)(4) (requiring telecommunications carriers to be capable of "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.").

154. Freeh, *supra* note 28, at 3.

155. *Id.*

156. *See* 47 U.S.C. § 1002 (a).

157. *See* 47 U.S.C. § 153; *see also* 47 U.S.C. § 1002.

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

159. *Id.* at 235-36.

160. *Id.* at 236.

that their equipment and facilities are capable of expeditiously isolating and enabling law enforcement "to access call-identifying information" and deliver "intercepted communications and call-identifying information to the government, pursuant to a court order or other lawful authorization."[161] The call-identifying information required is the "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."[162] In addition to call-identifying information, telecommunications providers are required to deliver call content.[163]

These requirements were to be built into or added onto the existing PSTN framework.[164] This addition to the architecture was performed with median difficulty by using functions like the conference calling features of the switches and adapting them to allow conference calls with silent listeners.[165] With this change in wiretap implementation, CALEA effectively allowed law enforcement to obtain additional information not available to taps on the local loop.[166] These wiretaps garner more information for law enforcement officers by allowing them to view information previously unavailable to them using wireline taps.[167] Under CALEA "the information available to the switch—call forwarding information, speed dial lists, [and] true caller identities . . ." are all available to the wiretap.[168] Though compliant wiretaps obtain more information and require less work by telecommunication companies, they cost law enforcement ten times more than traditional taps.[169] Despite the costs, compliant wiretaps are

---

161. 47 U.S.C. § 1002(a)(2)-(3).

162. *Id.* § 1001(2).

163. *Id.* § 1002(a)(3).

164. *See* U.S. CALEA MARKET INSIGHT 2 (2003). http://www.corp.att.com/stateandlocal/docs/US_CALEA_Market_Insight.pdf.

165. BELLOVIN ET AL., *supra* note 9, at 5-6 ("By requiring that digitally-switched networks be built in accordance with federal specifications for wiretapping, CALEA changed the design process.").

166. *Id.* at 5.

167. *Id.*

168. *Id.*

169. OFFICE OF THE INSPECTOR GEN., U.S. DEP'T OF JUSTICE, IMPLEMENTATION OF THE COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT: AUDIT REPORT 06-13 at xiii (2006), *available at* http://www.usdoj.gov/oig/reports/FBI/a0613/final.pdf, [hereinafter OIG AUDIT] ("A traditional wiretap costs law enforcement about $250. However, . . . a wiretap with CALEA features costs law enforcement approximately $2,200, according to law enforcement officials and carrier representatives . . . .").

substantially more efficient than previous methods.[170] Implementation of CALEA on the PSTN is essentially straightforward because it requires that all central office switches conform to a single standard.[171] This method of requiring conformity will not work for VoIP systems as they currently stand.[172]

C. Wiretap Legislation in the United Kingdom and Wiretap Examples from Europe

Though the United States limits its use of wiretaps to serious crimes,[173] other nations do not share the same standards.[174] There are substantially more wiretaps performed in Europe than in the United States with less oversight and fewer privacy protections.[175] The European Union Police Cooperation Working Group considered tagging each user of a satellite communications network because of the possibility of necessary surveillance issues.[176] British wiretapping is not a function of the judiciary at all, because the home secretary, a Cabinet minister, approves all wiretaps without a judge's opinion.[177] In 2001, English cabinet ministers authorized over 3400 wiretaps.[178] This figure excludes wiretaps in Northern Ireland, which have never been reported by the Interception of Communications Commissioner Report.[179] France surpasses England with over 4600 wiretaps authorized by the Commission Nationale De L'Informatique et des Libertes (CNIL) in 2002.[180] Requests for identification of cellular phone numbers were estimated in the same year at an average of 8000 to 25,000 requests per month.[181] Italian wiretaps have doubled every two years

170. *Id.* at 42 ("[A] New York law enforcement official noted that his agency can now initiate a wiretap on a wireless phone within a day. He also said that the carriers have greater capacity to conduct more wiretaps simultaneously.").

171. BELLOVIN ET AL., *supra* note 9, at 6.

172. *See id.*

173. DIFFIE & LANDAU, *supra* note 42, at 225.

174. *Id.*

175. Eric Weiner, *Wiretapping, European-Style. Think Bush's NSA Surveillance is Bad???* . . . .., TECHREPUBLIC.COM, Feb. 14, 2006, http://techrepublic.com.com/5208-6230-0.html?forumID=8&threadID=190272.

176. DIFFIE & LANDAU, *supra* note 42, at 225.

177. Weiner, *supra* note 175.

178. *See Surveillance of Communications Goes Through the Roof*, STATEWATCH.ORG, http://www.statewatch.org/news/2003/jan/11ukteltap.htm.

179. *Id.*

180. French Republic, Privacy International, http://www.privacyinternational.org/survey/phr2003/countries/france.htm (last visited Apr. 6, 2008).

181. *Id.*

since 2001, and in 2003 had a total of 77,000 requested wiretaps.[182] This boils down to 172 judicial intercepts in Italy in 2003 per 100,000 people in the country.[183] The United States authorized just over 1400 wiretaps in 2003,[184] but only denies an average of one or two wiretap requests per year.[185]

The European approach to wiretapping communications varies from country to country.[186] The United Kingdom takes an approach that is not followed by any other country in the world.[187] England's telecommunications surveillance statute is the Regulation of Investigatory Powers Act (RIPA)[188] The purpose of that statute is to allow the Security and Intelligence Services to conduct intelligence gathering for a number of uses, including disrupting operations.[189] RIPA gives the Security and Intelligence Services loosely defined terms and indicates that "authorised surveillance [is] lawful for all purposes."[190] For a law enforcement agency to obtain surveillance authorization, under the British statute, the request must be necessary on specified grounds and the surveillance must be proportionate to the goal to be achieved.[191] The statute requires that the authorizing official consider whether the information sought may be reasonably obtained by means other than intrusive surveillance.[192] Unlike United States surveillance authorizations, RIPA lists a series of officers with authority to authorize surveillance.[193] Not one of these authorized parties is a judge or judicial officer.[194]

This standard for obtaining a wiretap is lower than the narrowly focused requirements on United States law enforcement under CALEA, but there is yet another distinctive difference between United Kingdom and United States

---

182. *Italian GSM Provider Warns: Too Many Wiretaps*, EUROPEAN DIGITAL RIGHTS, Feb. 24, 2005, http://www.edri.org/edrigram/number3.4/wiretap.

183. *Id.*

184. *See* ADMIN. OFFICE OF THE U.S. COURTS, 2003 WIRETAP REPORT 15 tbl 2 (2003) *available at* http://www.uscourts.gov/wiretap03/Table2-03.pdf.

185. *See The Nature and Scope of Governmental Electronic Surveillance Activity*, CENTER FOR DEMOCRACY AND TECHNOLOGY, July 2006, http://www.cdt.org/wiretap/wiretap_overview.html.

186. *See* Keir Starmer, *Setting the Record Straight: Human Rights in an Era of International Terrorism*, 2 EUR. HUM. RTS. L. REV. 123, 129 (2007) (discussing surveillance systems in the United Kingdom).

187. *Id.*

188. Regulation of Investigatory Powers Act, 2000, ch. 23, § 1 (United Kingdom).

189. Starmer, *supra* note 186, at 129.

190. Amanda Hale & John Edwards, *Getting It Taped*, 12(3) COMP. & TELECOMM. L. REV. 71, 72 (2006) (discussing the impact of the Regulation of Investigatory Powers Act in the United Kingdom).

191. Regulation of Investigatory Powers Act § 32(2)(b).

192. *Id.* § 32(4).

193. *Id.* § 32(6)(a)-(n).

194. *See id.*

wiretaps.[195] Under RIPA sections 17 and 18, surveillance and wiretap evidence collected by law enforcement and the Security and Intelligence Services is *not* admissible in criminal prosecution.[196] Sections 17(1) and 17(1)(a) state "no evidence shall be adduced, question asked, assertion or disclosure made or other thing done in, for the purposes of or in connection with any legal proceedings . . . which . . . discloses . . . any of the contents of an intercepted communication or any related communications data."[197] Under this statute, the government can intercept data and compel a user to disclose the keys to unlock any encryption embedded within the intercepted data.[198]

Instead of taking steps to ensure that law enforcement can break encryption, or placing wiretaps in places that circumvent encryption, England has created a novel approach to wiretapping VoIP and other communications.[199] Part III section 49 of RIPA requires that if protected information (encrypted communications) comes into the hands of law enforcement, individuals or companies with encryption/decryption keys are required to surrender the keys to the communication or face jail time.[200] If law enforcement or a hacker has encryption/decryption keys, the encrypted communication is open for eavesdropping.[201]

The section containing the key disclosure requirement is broad.[202] Part III section 49 applies to protected information that:

> (a) has come into the possession of any person by means of the exercise of statutory power to seize, detain, inspect, search or otherwise to interfere with documents or other property, or is likely to do so; (b) has come into the possession of any person by means of the exercise of any statutory power to intercept communications, or is likely to do so; . . . [or] (e) has, by any other lawful means not involving the exercise of

---

195. *Compare* Starmer, *supra* note 186, at 129 *with* U.S. CONST. amend. IV *and* 47 U.S.C. § 1002 (a)(4)(2006).

196. *Id.*; *see also* Hale, *supra* note 190, at 73; *see also* Regulation of Investigatory Powers Act §§ 17-18.

197. Regulation of Investigatory Powers Act §§ 17(1)-(a).

198. *See Law Requiring Disclosure of Encryption Keys in Force*, OUT-LAW.COM, Oct. 2, 2007, http://www.out-law.com/default.aspx?page=8515.

199. *See* UK ST 2000 c. 23 Pt. III § 49 (Section forty-nine makes neither mention of breaking encryptions, nor placing wiretaps at specific locations. The section's importance revolves around the unique answer to encryption by requiring divulgence of encryption keys upon request by law enforcement.).

200. OUT-LAW.COM, *supra* note 198.

201. Nancy Gohring, *Zfone Encrypts VoIP for Windows Users but Doesn't Work with Skype*, PC ADVISOR, May 22, 2006, http://www.pcadvisor.co.uk/news/index.cfm?newsid=6219.

202. Ken Fisher, *UK Can Now Demand Data Decryption on Penalty of Jail Time*, ARS TECHNICA, Oct. 1, 2007, http://arstechnica.com/news.ars/post/20071001-uk-can-now-demand-data-decryption-on-penalty-of-jail-time.html.

> statutory powers, come into the possession of any of the intelligence services, the police . . . or is likely so to come into the possession of any of those services . . . .[203]

Law enforcement agents or agencies may impose a disclosure requirement to obtain the key, after possessing the information or if they are likely to intercept it.[204] The disclosure requirement is justified for national security purposes,[205] crime prevention or detection,[206] or "in the interests of the economic well-being of the United Kingdom."[207] These requirements essentially make it criminal to refuse to decrypt or hand over decryption keys for almost any encrypted data requested under the auspices of a terror or criminal investigation.[208]

The statute was intended to aid law enforcement in catching terrorists, pedophiles, and computer criminals.[209] However, the key possession requirement and disclosure request may simply force a criminal to choose whether to be charged for his alleged crime or charged for non-compliance with the request.[210] Once the disclosure request has been made, non-compliance can result in either a two or five year prison sentence,[211] even if the person is no longer in possession of the required keys.[212] Section 53(2) indicates that a person is in possession of a key:

> if it is shown that that person was in possession of a key to any protected information at any time before the time of the giving of the section 49 notice, that person shall be taken for the purposes of those proceedings to have continued to be in possession of that key at all subsequent times, unless it is shown that the key was not in his possession after the giving of the notice and before the time by which he was required to disclose it.[213]

Even though a person may be convicted of possessing and not disclosing a key when he does not have it, this section could be a blessing in disguise for certain criminals.[214] If a criminal has encrypted data, such as child pornography,

---

203. Regulation of Investigatory Powers Act, 2000, ch. 23, §§ 49(1)(a)-(e) (United Kingdom).

204. *Id.* § 49(2)(d).

205. *Id.* § 49(3)(a).

206. *Id.* § 49(3)(b).

207. *Id.* § 49(3)(c).

208. Fisher, *supra* note 202.

209. *Id.*

210. *Id.*

211. *See* Regulation of Investigatory Powers Act § 53(5)(a).

212. *See id.* § 53(2).

213. *Id.*

214. *See* Fisher, *supra* note 202.

he may have an easier time serving a sentence of two years for non-compliance than serving a longer sentence for a child pornography conviction.[215] Another hole in the legislation appears in the notice and non-compliance sections.[216] Recently, British law enforcement "invited" an animal rights activist to hand over a decryption key for encrypted data found on her confiscated hard drive.[217] It is unclear if the "invitation" is an official notice under section 49 of RIPA.[218] The potential for ineffectual notice and the evasion of punishment for a crime, by refusing to decrypt information, indicate there are flaws in the new legislation that will have unknown effects.[219]

D. Fourth Amendment and Privacy in Wiretapping

CALEA will either become an important first step to ensuring law enforcement agencies have tools to combat crime and promote security, or the efforts will extend too far, casting an unwelcome gaze onto the private communications of innocent citizens.[220] Wiretapping has become an important part of law enforcement capabilities since its first use in the early 1890s,[221] but must be balanced against the Fourth Amendment "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures . . . ."[222] Regardless of the benefits of RIPA, or the standards for wiretaps used in the European Union, United States citizens are entitled to privacy against unreasonable searches and seizures unless a warrant is issued "upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the person or things to be seized."[223]

Though there may be a temptation to implement CALEA capabilities at a residential gateway,[224] and potentially subject massive numbers of communications to wiretap interceptions,[225] it is important to maintain privacy

---

215. *Id.*

216. *See* John Leyden, *Animal Rights Activist Hit with RIPA Key Decrypt Demand*, THE REGISTER, Nov. 14, 2007 http://www.theregister.co.uk/2007/11/14/ripa_encryption_key_notice/.

217. *Id.*

218. *Id.*

219. *See id.*; *see also* Fisher, *supra* note 202.

220. *See* FED. COMMC'NS COMM'N, FIRST REPORT AND ORDER AND FURTHER NOTICE OF PROPOSED RULEMAKING, FCC 05-153, 55 (2005) (statement of Commissioner Michael J. Copps), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-05-153A1.pdf [hereinafter FCC REPORT].

221. DIFFIE & LANDAU, *supra* note 42, at 177.

222. U.S. CONST. amend. IV.

223. *Id.*

224. *See* DIFFIE & LANDAU, *supra* note 42, at 221-22.

225. *Id.*

standards and the narrow and tailored nature of wiretaps currently in force.[226] The tailoring of wiretap applications includes a written statement including an oath or affirmation to the judge of competent jurisdiction.[227] The application must also contain:

> a full and complete statement of the facts and circumstances relied upon by the applicant, to justify his belief that an order should be issued, including (i) details as to the particular offense . . . (ii) . . . a particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted, (iii) a particular description of the type of communications sought to be intercepted, (iv) the identity of the person, if known, committing the offense . . . .[228]

Though wiretap applications and implementation must be narrow and specified, and despite the privacy and oversight structures in place, "[w]hen a government has the power to invade privacy, abuses occur."[229]

The temptation to infringe on liberties in order to maintain national security was observed by Niccolo Machiavelli.[230] Machiavelli stated "when the well-being of one country is at all in question, no consideration of justice or injustice, of mercy or cruelty, of honour or shame must be allowed to enter."[231] Although compelling, Machiavelli's interest in national security would extend not only to outside invaders but to potential threats within a nation.[232] This view would override the purpose of the Fourth Amendment, which is "to protect the people of the United States against arbitrary action[s] by their own Government . . . ."[233]

Under the Fourth Amendment and applicable statutes, U.S. courts wavered in their support of wiretaps.[234] In *Olmstead v. United States*, circa 1928, the Supreme Court upheld the use of warrantless wiretaps in criminal cases.[235] The five justices of the majority indicated that the Fourth Amendment protected only

---

226. *See* 18 U.S.C. § 2518 (2006).

227. *Id.* § 2518(1).

228. *Id.* § 2518(1)(b).

229. DIFFIE & LANDAU, *supra* note 42, at 169.

230. STERLING JOHNSON, GLOBAL SEARCH AND SEIZURE: THE U.S. NATIONAL INTEREST V. INTERNATIONAL LAW 1 (1994).

231. *Id.*

232. *See* NICCOLÒ MACHIAVELLI, THE PRINCE AND OTHER WRITINGS, 196-97 (Wayne A. Rebhorn trans., Barnes & Noble Books 2003) (Machiavelli's notion that the well-being of a country is above considerations of morality, cruelty, and injustice for enemies of national security readily applies to citizens of the country when he writes, ". . .there must be a memorable punishment of those who are the enemies of the present state of affairs.") *Id.* at 196.

233. United States v. Verdugo-Urquidez, 494 U.S. 259, 266 (1990).

234. *See* DIFFIE & LANDAU, *supra* note 42, at 177-79,189-94 .

235. *See* Olmstead v. United States, 277 U.S. 438, 464 (1928).

tangible objects, and that conversations were not protected.[236] Nine years later in *Nardone v. United States*, the Supreme Court ruled that, under the Federal Communications Act of 1934 (FCA),[237] wiretaps initiated by federal agents were not admissible as evidence in a criminal proceeding.[238] In a second case involving *Nardone*, the court decided that evidence derived from warrantless wiretaps was also inadmissible.[239] Finally, the Supreme Court in *Weiss v. United States*, decided that the FCA applied to, and excluded, wiretap evidence from interstate and intrastate communications.[240] After these decisions, Attorney General Robert Jackson ordered a cessation of FBI wiretapping.[241] In 1940, this prohibition was overridden by President Roosevelt, at the behest of J. Edgar Hoover, for national security purposes.[242] Even though the prohibition was lifted for national security reasons, it was not until the Omnibus Safe Streets and Crime Control Act that Congress made it legal for law enforcement to wiretap with a warrant.[243]

V. THE DIFFERENCE BETWEEN SEEING AND KNOWING

It is possible to track an encrypted communication between two IP addresses, even if one is unknown.[244] It is impossible, however, to listen to the content of an encrypted VoIP communication without breaking or undermining the encryption.[245] Because of the inherent difficulties in wiretapping packet switched networks, and the need to break encryptions, law enforcement agencies need a more tailored method for obtaining wiretaps other than the original wireline or CALEA model.[246] However, this tailored method should not take the form of a back door into encrypted systems.[247]

---

236. *Id.*

237. The Communication Act of 1934 created the Federal Communications Commission and gave it regulating authority over radio and wire for interstate and international communications. 47 U.S.C. § 151-52; *see also* About the FCC, http://www.fcc.gov/aboutus.html (last visited Apr. 7, 2008).

238. Nardone v. United States, 302 U.S. 379, 384 (1937).

239. *See* Nardone v. United States, 308 U.S. 338, 340-41 (1939).

240. *See* Weiss v. United States, 302 U.S. 321, 329 (1939).

241. DIFFIE & LANDAU, *supra* note 42, at 179.

242. *Id.* at 179.

243. *Id.* at 193-95.

244. *See* WANG ET AL., *supra* note 67.

245. *Id.*

246. *See* BELLOVIN ET AL., *supra* note 9, at 11-15.

247. SCHNEIER, *supra* note 74, at 9.

A. Why Packet Switching Impedes Wiretap Capabilities

Even if the communication is not encrypted, packet switch networks create potential difficulties to wiretapping communications.[248] Some types of VoIP communications work solely on a packet switching network.[249] If the communication takes a defined static path through a communication network, the call may be easily intercepted and recorded by placing a tap between two switches or routers along that path.[250] The fundamental flaw in this system of wiretapping is that packets do not always travel down the same path in a network, even if the source and destination addresses do not change.[251] United States Patent 7,055,174 considers the problem of different packet routes and answers the problem by placing the wiretapping system at the first network node.[252] This is tantamount to the original wireline method of placing a tap within the last mile, near the local loop.[253] There is still a problem with this type of wiretapping: wireless communication towers.[254]

At a typical home with a wireless router, wiretapping at the first network node poses no great risk of exposing law enforcement wiretaps, yet this is potentially the least likely place for a crime committed over VoIP.[255] Cities like London and New York have thousands of wireless access points[256] and have repeatedly been the focus of terrorist attacks.[257] This year, New York City boasts 6371 wireless access points along the survey route, and London 7130.[258]

---

248. *See* BELLOVIN ET AL., *supra* note 9, at 14-15.

249. GOLENIEWSKI, *supra* note 8, at 92-93.

250. *See* U.S. Patent No. 7,055,174 para. 1 (filed Feb. 26, 2001), *available at* http://www.patentstorm.us/patents/7055174-claims.html, [hereinafter Patent 7,055,174] (last visited Apr. 7, 2008); *see also* FreePatentsOnline, http://www.freepatentsonline.com/20060018255.html, [hereinafter Free Patents] (last visited Apr. 7, 2008).

251. GOLENIEWSKI, *supra* note 8, at 96.

252. *See* Patent 7,055,174, *supra* note 250, para. 10.

253. *See* BELLOVIN ET AL., *supra* note 9, at 5.

254. *See* Metzger, *supra* note 23.

255. *See generally* DANILO YANICH, CRIME CREEP: URBAN & SUBURBAN CRIME ON LOCAL TV NEWS 14 (2004).

256. RSA SECURITY, THE WIRELESS SECURITY SURVEY OF NEW YORK CITY 2 (3d ed. 2007), *available at* http://www.rsa.com/solutions/wireless/survey/wireless_security_survey_nyc_2007.pdf, [hereinafter SURVEY OF NEW YORK].

257. *See* Maria Godoy, *Timeline: London's Explosive History*, NPR.org, July 7, 2005, http://www.npr.org/templates/story/story.php?storyId=4734400; *see e.g.* Meyer Berger, *Bomber is Booked; Sent to Bellevue for Mental Tests*, N.Y. TIMES, Jan. 23, 1957, at 1; Douglas Jehl, *A Tool of Foreign Terror, Little Known in the U.S.*, N.Y. Times, Feb. 27, 1993, at 24; Robert D. McFadden, *A Grim Forecast*, N.Y. TIMES, Sept. 13, 2001, at A1.

258. SURVEY OF NEW YORK, *supra* note 256, at 2.

Though only twenty-four percent of the access points in New York are unsecured, and nineteen percent in London,[259] that still leaves more than 1500 access points available for misuse in New York, and more than 1300 in London. There are currently groups such as NYC wireless that seek to promote and further expand the already pervasive free wireless access in major cities.[260]

If properly configured, a communication can change wireless access points in the middle of the communication without any substantial effect on the conversation.[261] This requires law enforcement to track the geographic position of the mobile VoIP source, tap all of the available wireless access points in the vicinity, or place the wiretap closer to the source of the communication.[262] Tapping numerous access points or tracking and changing the location of the tap quickly poses problems with the minimization requirements of CALEA,[263] where law enforcement must ensure minimal eavesdropping on communications and communications channels not within the scope of the warrant.[264] The problem of discovery arises from having to place a wiretap closer to the mark.[265] With the possibility of constantly changing the access point and packet path through the network, law enforcement agencies lose the valuable asset of an attenuated choke point.[266] CALEA sought to use these choke points, nodes through which all communications must pass, to allow law enforcement to wiretap in comfort.[267] As the choke point for communications comes closer to the source of the communications, the risk of detection becomes greater.[268]

The final underlying problem with the packet switch network and the elimination of choke points is the right and opportunity of law enforcement to access the VoIP user's machine.[269] In an effort to exploit these choke points, the FBI used a system called Carnivore to monitor email, file transfers, and web

---

259. *Id.* at 3.

260. Tom Vanderbuilt, *Walker in the Wireless City*, N.Y. TIMES, Nov. 24, 2007, at CY 1.

261. Free Patents, *supra* note 250. (United States Patent 20,070,047,516).

262. *See* DIFFIE & LANDAU, *supra* note 42, at 298.

263. *See* Steven Bellovin, *Wiretapping the Net*, The Bridge, Vol. 30, Num. 2, Summer 2000, *available at* http://www.nae.edu/nae/bridgecom.nsf/weblinks/NAEW-4Q6TS8?OpenDocument. [hereinafter *Wiretapping the Net*].

264. Communications Assistance for Law Enforcement Act, 47 U.S.C. § 1002.

265. *See* DIFFIE & LANDAU, *supra* note 42, at 295-99.

266. *Id.*

267. *Id.* at 220-21.

268. *Id.* at 298.

269. *See* John Birbeck, *A New Record*, COMMSBUSINESS, http://www.commsbusiness.co.uk/Comms_Business_Feature.cfm?FeatureID=234(last visited Apr. 8, 2008).

browsing without warrants.[270] The use of the system has fallen by the wayside after public and political outcry, and after more effective commercial options surfaced.[271] The program moved a step past CALEA and allowed the FBI the capability of massive simultaneous wiretapping.[272] Carnivore was intended to gather all information or specific information that passed through a given Internet Service Provider (ISP).[273] The system could be set up to either fully wiretap or identify specific conversations which would not eavesdrop on the content of the Internet traffic.[274] Carnivore created public outcry due to its obvious intimidating name, and its ability to read and copy large amounts of communications.[275] The FBI's initial use of CALEA telephone architecture enabled it to eavesdrop and record over 57,000 communications lines simultaneously.[276] Though the ability of the FBI's use of Carnivore leads to impressive numbers, CALEA requires law enforcement to minimize the communications they intercept to those specifically enumerated in the warrant.[277] The FBI can open its capabilities and swallow large amounts of communications, but trouble still revolves around staying within the auspices of the wiretap warrant while tracing packets that take separate routes when both end points are not known.[278]

B. Peer-to-Peer Communications Will Often Evade Detection of Law Enforcement

Peer-to-peer communications are fundamentally different from other VoIP communications.[279] VoIP communications all begin with protocols that act as a

---

270. *See* STEPHEN P. SMITH ET AL., INDEPENDENT TECHNICAL REVIEW OF THE CARNIVORE SYSTEM, ILLINOIS INSTITUTE OF TECHNOLOGY RESEARCH INSTITUTE viii (2000) http://www.usdoj.gov/archive/jmd/carniv_final.pdf.

271. *See* DIFFIE & LANDAU, *supra* note 42, at 269-71.

272. *See Id.*

273. *Id.* at 269.

274. *See* SMITH ET AL., *supra* note 270, at viii.

275. *Id.*

276. *Id.*

277. Communications Assistance for Law Enforcement Act, 47 U.S.C. §1002 (a)(1) reads in part:

> [a] telecommunications carrier shall ensure that its equipment, facilities, or services . . . 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 . . . .

Id.

278. *See generally* WANG ET AL., *supra* note 67, at 1-3; *See also Wiretapping the Net*, *supra* note 263.

279. *See* OFCOM, *supra* note 46, at 7-8.

handshake between the two users that begins a conversation.[280] Peer-to-peer communications differ from other conversations because they have little use for the ISP or the provider network.[281] After the handshake, these communications use packet routing determined by the conversing parties or occasionally, by the provider, such as Skype.[282] Because peer-to-peer connections do not use the PSTN, their connections cannot be wiretapped by the usual means.[283]

If an eavesdropper wishes to attack a peer-to-peer communication, he would naturally place his tap as near as possible to the originating Internet connection, like the home router or initial junction between the Internet cable and the rest of the network.[284] This method, however, does not benefit law enforcement.[285] The individual routers or initial Internet connections are unintelligent.[286] The routers cannot tell the difference between one type of communication and another.[287] Therefore, law enforcement would have to require the ISP from each party to the conversation send a signal indicating when to begin recording to ensure the conversation is being captured rather than random Internet traffic.[288]

Even if the ISP could give timely notice to law enforcement, the ISP would still not catch all the peer-to-peer communications.[289] These communications are not limited, as some other VoIP styles, to physical phone equipment or specific hardware and software requirements.[290] Asterisk is one such peer-to-peer VoIP communication program.[291] Each Asterisk user is involved in the programming and implementation of his own Asterisk program.[292] The creation of one of these programs may be as simple or as encrypted and complex as the user desires.[293] Because these programs do not go through normal channels, and only require an Internet connection, Asterisk users can maneuver easier in an

280. TED WALLINGFORD, SWITCHING TO VOIP 12 (Michael K. Loukides ed., O'Reilly 2005).

281. *Id.*

282. BELLOVIN ET AL., *supra* note 9, at 3-4.

283. *Id.*

284. *Id* at 5.

285. *Id.*

286. DIFFIE & LANDAU, *supra* note 42, at 296-97.

287. *Id.*

288. *Id.*

289. *Id.* at 298.

290. JIM VAN MEGGELEN ET AL., ASTERISK: THE FUTURE OF TELEPHONY 9 (Michael K. Loukides ed.,O'Reilly 2005).

291. *Id.*

292. *Id.* at 5.

293. *Id.* at 10.

environment where peer-to-peer providers may track movements for law enforcement.[294]

C. Encryption: Why it Could be Impossible to Know What VoIP Conversations Involve

In order to discover the contents of an Internet communication, an eavesdropper must capture the conversation in real-time or near real-time because the data packets for VoIP are not stored like those of an email.[295] If a communication is not encrypted, an eavesdropper can use tools freely available on the Internet to capture and record calls.[296] One such program is called Voice Over Misconfigured Internet Telephones (VOMIT).[297] However, if the communication is encrypted, the difficulties for the eavesdropper rise literally at an exponential rate.[298] If a VoIP communication employs a public key encryption system, it could take an eavesdropper with access to Cray[299] computers an infeasible amount of time to break the secret key used for decoding the message.[300] A real world example of this took place in 2002 when 331,000 volunteers cracked a sixty-four bit cipher after four years of computing.[301] A sixty-four bit cipher key requires 2^{64} possible key values.[302] If a cipher key is 128 bit, as is the current standard, it would require somewhere in the realm of 2^{128} processes to break the algorithm.[303] To place the difficulty in perspective, the possibility of winning the grand prize in a state lottery in the United States and being killed by a lightning strike in the same day are 1 in 2^{55}, and 2^{170} represents the number of atoms in the planet.[304]

---

294. *See* Y.J. LIANG, ET AL., MULTI-STREAM VOICE OVER IP USING PACKET PATH DIVERSITY 4, Appearing in 2001 Fourth Workshop on Multimedia Signal Processing) (IEEE 2001), *available at* http://www.stanford.edu/~bgirod/pdfs/mmsp.pdf.

295. Kim Zetter, *Privacy Guru Locks Down VoIP*, WIRED, July 26, 2005, http://www.wired.com/science/discoveries/news/2005/07/68306?currentPage=1.

296. DAVID ENDLER & MARK COLLIER, HACKING EXPOSED VOIP: VOICE OVER IP SECURITY SECRETS AND SOLUTIONS 160-65 (2007)

297. *Id.*

298. *See* SCHNEIER, *supra* note 74, at 31.

299. "The Cray T3E-1200E™ system [debuting in 1995] was the first supercomputer to sustain one teraflop (1 trillion calculations per second) on a real world application." Cray History, http://www.cray.com/about_cray/history.html (last visited Apr.8, 2008).

300. SCHNEIER, *supra* note 74, at 31.

301. Dennis Fisher, *Team Cracks RSA Encryption Challenge*, EWEEK.COM, Sept. 27, 2002, http://www.eweek.com/article2/0,3959,560039,00.asp.

302. FERGUSON & SCHNEIER, *supra* note 76, at 34.

303. SCHNEIER, *supra* note 74, at 9; *see also* FERGUSON & SCHNEIER, *supra* note 76, at 43.

304. SCHNEIER, *supra* note 74, at 18.

The effectiveness of cryptography does not require that a key be unbreakable.[305] The measure of effectiveness for a given cipher is whether it is computationally secure (i.e. it cannot be broken with current or future estimated available resources).[306] In its simplest form, the security of an algorithm can be understood as a balance between the time required to break the algorithm and the time the encrypted data must remain secret.[307] Crime is often time sensitive.[308] The FBI recognizes that terrorist attacks, bombings, kidnappings, and repetitive violent crimes are among the most time sensitive crimes.[309] Using an encryption method even as low as the fifty-six bit key encryption in DES could cost the government up to one million dollars to break the simple encryption in ten days.[310] DES is on the edge of what current technology can break with its fifty-six bit encryption, however, the standard key length is currently 128-bit.[311] It is not possible to determine the time required to break a 128-bit encryption based on the ten-day figure for fifty-six bit encryption as the difference in possible combinations between the two, 2^{56} to 2^{128}, is an exponential difference.[312] With a possible decryption time of ten days to thirty years, the value of time sensitive data is likely to be lost.[313]

D. The Effect of the FCC Deadline for Wiretap Capabilities on the United States

The Federal Communications Commission (FCC) required VoIP wiretap capability enhancements were to be completed by May 2007.[314] Though the Act covered all broadband Internet service providers, it was not immediately forced on libraries[315] or universities.[316] Both libraries and universities opposed the

---

305. *See id.* at 8.

306. *Id.*

307. *Id.*

308. *See* FBI, Investigative Programs Critical Incident Response Group, http://www.fbi.gov/hq/isd/cirg/mission.htm (last visited Apr. 7, 2008).

309. *Id.*

310. Michael Anderson, *Internet Security – Firewalls & Encryption the Cyber Cop's Perspective*, NEW TECHNOLOGIES INC., http://www.forensics-intl.com/art1.html.(last visited Apr. 8, 2008).

311. *Id.*

312. SCHNEIER, *supra* note 74, at 9.

313. *See* FERGUSON & SCHNEIER, *supra* note 76, at 37.

314. Nate Anderson, *CALEA Deadline Arrives: US VoIP, Broadband Must Be Wiretap-Friendly*, ARS TECHNICA, May 14, 2007, http://arstechnica.com/news.ars/post/20070514-calea-deadline-arrives-us-voip-broadband-must-be-wiretap-friendly.html.

315. ALBERT GIDARI, OFFICE FOR INFO. TECH. POLICY AND AM. LIBRARY ASS'N, THE COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT (CALEA) AND LIBRARIES 3 (2007), *available at* http://www.ala.org/ala/washoff/woissues/techinttele/calea/caleajan07.pdf.

legislation due to the potential for high costs.[317] Under the Act, if a university or library obtains Internet access through a facilities-based provider, the university or library has no CALEA obligations.[318] However, if a library obtains Internet access via a regional or local network, a private network, or an academic institution, the library is subject to wiretap compliance.[319] Because of the potential cost to libraries and universities, and the power of the FCC to exempt specific telecommunications carriers from compliance, library and university associations have urged the FCC to consider their exemption from compliance.[320]

If libraries and universities become exempt from CALEA compliance, it only saves money, not the potential sacrifice in privacy.[321] In order to avoid the cost of compliance, some universities have opted to stop offering public Internet access.[322] Regardless of their status under the Act, libraries and universities are subject to government wiretap requests.[323] Although the institutions may not have CALEA compliant facilities, if they obtain Internet access through a broadband service provider, communications within the university and library network can still be accessed using the interception capabilities through the service provider.[324]

CALEA does have a safe harbor section that allows a maximum extension of two years of the compliance deadline.[325] The safe harbor provision allows a telecommunications carrier to petition for an extension if it has tried or is currently implementing the required capabilities.[326] If petitioned, the FCC and the Attorney General determine whether compliance is not reasonably achievable through available technology within the compliance period.[327] Though the extension may be granted more than once, the extension only applies

316. Nate Anderson, *CALEA: It Doesn't Apply to Universities and Libraries After All*, ARS TECHNICA, May 17, 2007, http://arstechnica.com/news.ars/post/20070517-calea-it-doesnt-apply-to-universities-and-libraries-after-all.html.

317. *Id.*

318. GIDARI, *supra* note 315, at 3; *see also* Anderson, *supra* note 312.

319. GIDARI, *surpa* note 315, at 3.

320. *Id.* at 3-4.

321. *See generally* Anderson, *supra* note 314 (discussing the costs required to upgrade infrastructure in libraries and universities if not exempted and the fact that both groups are still required to comply with government wiretap requests regardless of any exemption).

322. *Id.*

323. *Id.*

324. GIDARI, *surpa* note 315, at 3.

325. Communications Assistance for Law Enforcement Act, 47 U.S.C. §§ 1006 (c)(3) (1994).

326. *Id.* § 1006(c)(1).

327. *Id.* § 1006(c)(2).

to those parts of the telecommunication carrier's business on which the new technology or compliance equipment is used.[328]

VI. DIFFERENCES BETWEEN WIRETAPPING POLICIES IN THE UNITED KINGDOM AND THE UNITED STATES, AND THE IMPLEMENTATION OF VOIP WIRETAPPING.

A. The Danger to Privacy from CALEA and Blanket Implementation of Wiretapping Capabilities

CALEA contains security and integrity requirements to protect the privacy of callers who are not subject to law enforcement wiretaps and to all callers when law enforcement personnel are not actively tapping communications.[329] Outlining the system security and integrity demands, the Act requires that:

> [a] telecommunications carrier shall ensure that any interception of communications or access of call-identifying information effected within its switching premises can be activated only in accordance with a court order or other lawful authorization and with the affirmative intervention of an individual officer or employee of the carrier acting in accordance with regulations prescribed by the Commission.[330]

Though section 1004 requires the communications carrier to ensure activation only in accordance with a court order, the FBI has recognized and sought to address additional areas of security breaches.[331] The FBI has specifically petitioned the FCC to amend CALEA to include personnel security measures and a measure requiring telecommunications carriers to report events that are suspected to have compromised the security of the system.[332] It also petitioned to add a section requiring the telecommunications carriers to record the initiation of call interceptions.[333] Finally, the FBI requested the FCC reconsider a rejected amendment that would establish automated surveillance

---

328. *Id.* § 1006(c)(4).

329. *See id.* § 1004.

330. *Id.*

331. *See* Commc'ns Assist. for Law Enforcement Act, 16 F.C.C.R. 8959, 8960 (2001).

332. *Id.* at 8960; *see generally* BELLOVIN ET AL., *supra* note 9, at 12 n.5 (explaining that the FBI's concerns about security measures are in part warranted by a wiretapping scandal where an unknown insider at Vodafone Corporation implemented a CALEA-like wiretap technology created by Ericsson that intercepted the communications of Greek government ministers); *see also* John Leyden, *Vodafone Fined €76m Over Greek Wiretap Scandal*, THE REGISTER, Dec. 15, 2006, http://www.theregister.co.uk/2006/12/15/voda_fined_over_greek_wiretaps/ (explaining that the cellular phone calls of Costas Karamanlis, the Prime Minister of Greece, were also illegally monitored).

333. Commc'ns Assist., 16 F.C.C.R. at 8960.

status messages.[334] Though the Commission rejected the proposals for increased security measures and tracking measures for call interceptions,[335] the Chairman of the FCC, Kevin J. Martin, indicated that the Commission will "continue [to work] . . . to address and overcome any challenges that stand in the way of effective lawful electronic surveillance."[336] In the same statement, Martin said, "[r]esponding to the needs of law enforcement is of paramount importance."[337]

Aside from ignoring potential security risks, CALEA also potentially requires a change in VoIP technology.[338] Once initiated, communications traffic flows directly between the two ends of the call.[339] The call does not continue to travel through the VoIP provider,[340] and it does not have to travel continuously through the same path between the two ends of the connection.[341] One way law enforcement could obtain wiretaps over a packet network is to require a provider to direct traffic through a law enforcement intercept point.[342] This option would likely require the assistance and cooperation of a sizeable segment of the routing infrastructure.[343] Though directing the packet traffic would allow law enforcement better access and ability to wiretap VoIP calls, it also allows others access to the same traffic at the same point.[344] Hacking into VoIP communications has been the subject of much discussion.[345] After the hacker has access to the network and communication, his job is made easier by many tools designed to intercept and record Internet traffic.[346] By channeling the communication through specific networks and routers, the CALEA accommodations give easy access to law enforcement and hackers alike.[347] In fact, the Swiss Department of the Environment, Transport, Energy and Communications is examining the viability of using spyware[348] to enable it to tap VoIP communications.[349]

---

334. *Id.*

335. *Id.* at 8960-66.

336. FCC REPORT, *supra* note 220, at 53 (statement of Chairman Kevin J. Martin).

337. *Id.*

338. *See* BELLOVIN ET AL., *supra* note 9, at 6-7.

339. *Id.* at 6.

340. *Id.*

341. *See* GOLENIEWSKI, *supra* note 8, at 96.

342. BELLOVIN ET AL., *supra* note 9 at 12.

343. *Id.* at 13.

344. *Id.*

345. *See generally* ENDLER, *supra* note 296 (Jane K. Brownlow ed., McGraw Hill 2007) (illustrating the example that entire books have been on the subject and measures to prevent it.).

346. *Id.* at 160-64.

347. *See* BELLOVIN ET AL., *supra* note 9 at 13.

348. PCMag.com, http://www.pcmag.com/encyclopedia_term/0%2C2542%2Ct%3Dspyware&i%3D51898%2C00.as

CALEA presents a further potential impact on privacy because of the nature of Internet traffic.[350] The Act makes no differentiation in the type of electronic communication that is subject to lawful wiretap.[351] Capturing conversations on packet switch networks in real time means having to place the wiretap as near as possible to the source or destination.[352] Because packets are not differentiated, this requires either hardware or software capable of trapping all Internet traffic coming through the designated choke point.[353] If the choke point is tapped in this way, not only will the call be intercepted, but also all of the other traffic from that Internet connection.[354] Although trapping all the Internet traffic from one suspect connection could be justified under the current wiretapping standards, the placement of the choke point could also mean that all the traffic through a larger residential gateway is accessed, including the specified connection and all others in the neighborhood.[355]

CALEA is specific in its function, however, requiring telecommunications carriers to build wiretap capabilities into the systems.[356] Though this could limit the need to tap an entire neighborhood's Internet gateway connection, it intentionally places holes in a system.[357] The privacy protection allowed by this method, as opposed to the gateway tap, presents opportunities for law enforcement and hackers alike.[358] As an alternative to requiring a telecommunications provider to put intentional interception capabilities in a system, CALEA allows a telecommunications provider to outsource its compliance to a trusted third party.[359] This technique requires routing traffic

---

p (last visited Apr. 8, 2008)(defining Spyware as "[s]oftware that sends information about your Web surfing habits to its Web site. . . . [S]pyware transmits information in the background as you move around the Web.").

349. John Leyden, *Swiss Gov 'Mulls' Spyware to Tap VoIP Calls*, THE REGISTER, Oct. 10, 2006, http://www.theregister.co.uk/2006/10/10/swiss_voip_wiretap_plan/ (explaining that a Swiss firm, ERA IT Solutions, is attempting to keep its software, Superintendent Trojan, away from anti-virus and anti-spyware lists, which commonly detect and eliminate spyware, by solely providing access to the software to government agencies).

350. *See* BELLOVIN ET AL., *supra* note 9, at 13.

351. *Id.*; *see also* Communications Assistance for Law Enforcement Act, 47 U.S.C. § 1001-10 (2006).

352. Andrew Brandt, *Privacy Watch: Listening in to Net Phone Conversations*, PC WORLD, Sept. 29, 2004, http://www.pcworld.com/printable/article/id,117800/printable.html.

353. *Id.*

354. *Id.*

355. *Id.*

356. *See* 47 U.S.C. §§ 1002-06.

357. *See* Brandt, *supra* note 352.

358. *Id.*

359. Anderson, *supra* note 310.

through the third party.[360] As explained in the previous section, routing traffic through a specific point creates just as much vulnerability to eavesdropping by law enforcement as by hackers.[361] Regardless of third party routing, or built-in compliance, because CALEA fails to address end-user encryption, it will be of limited use as encryption by subscribers or end-users of VoIP communications becomes more commonplace.[362]

B. The Need for Careful Legislation in the United States and Europe

CALEA has been "undeniably stretched to recognize new service technologies and pushed very hard to accommodate new and emerging telecommunications platforms."[363] The Act may require further stretching, however, because the proposed rulemaking that expands it does not include peer-to-peer communications.[364] The proposed rulemaking separates VoIP into two categories: managed and non-managed.[365] Peer-to-peer communications fall under the non-managed category that escapes compliance requirements.[366] The distinction arose because peer-to-peer providers maintain minimal or no involvement in packet flow during the communication.[367] The distinction removes Skype and other peer-to-peer providers from CALEA's purview, and in turn, eliminates the largest segment of VoIP subscribers from the wiretap requirements.[368] Although some may think the Act's expansion means criminals and terrorists who switch to VoIP will be easily caught, if they switch to a non-managed or peer-to-peer communication, they will not have to worry about built in interception technology.[369] The peer-to-peer exclusion combined with the potential for encryption seems to denote a potential problem for law enforcement wiretaps.[370]

---

360. *Id.*

361. BELLOVIN ET AL., *supra* note 9 at 13.

362. 47 U.S.C. § 1002; *see also* Gohring, *supra* note 201.

363. FCC Report, *supra* note 220, at 55.

364. *See* FED. COMMC'NS COMM'N, NOTICE OF PROPOSED RULEMAKING AND DECLARATORY RULING, FCC 04-187, 18-20, *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-04-187A1.pdf [hereinafter FCC PROPOSED RULE].

365. *Id.*

366. *Id.*

367. *Id.*

368. Skype Hits 100M, *supra* note 26.

369. FCC PROPOSED RULE, *supra* note 364, at 19.

370. Gohring, *supra* note 201; *see generally* Shiping Chen et al., *On the Anonymity and Traceability of Peer-to-Peer VoIP Calls,* 20 IEEE NETWORK: THE MAGAZINE FOR GLOBAL INTERNETWORKING, Sept.- Oct. 2006, at 32-37.

Although VoIP calls may be traced even while encrypted, the call content remains obscured from the view of law enforcement.[371] If the caller is able to encrypt the communication, the call content will be confidential.[372] Though the call may be traced, and call identifying information gathered, the call content cannot be determined without the encryption keys,[373] unless the encryption is broken.[374] This is where legislation like RIPA comes into play.[375] RIPA allows British law enforcement and intelligence services to demand decryption keys for information residing in the UK, on English servers, or devices in Britain.[376] However, the UK statute still does not allow information gained in lawful interceptions to be used in court.[377] There is a danger in this sort of legislation, even if the information is not allowed in court.[378] Because of the danger of abuse, legislation of this nature is likely to have an effect on the economy.[379] International corporations and banks would be justifiably nervous if their encryption could be compromised with a simple form request for disclosure.[380]

The two fundamental differences between RIPA and CALEA create the greatest need for careful legislation.[381] RIPA cannot be used in court as evidence.[382] It can however, be used to require encryption/decryption keys from either the criminal involved or any other party who may have the encryption/decryption keys.[383] CALEA interceptions may be used in court, but United States law enforcement agencies have no authority to demand encryption/decryption keys from the possessing parties.[384] The right to demand encryption/decryption keys has privacy implications that rival the privacy problems of building back door wiretap capabilities into VoIP

371. CHEN ET AL., *supra* note 370, at 33.

372. *Id.*

373. *See e.g.* Gohring, *supra* note 201 (showing Zfone as an example of one VoIP encryption method that protects encryption keys from those not party to the communication, making the encryption more difficult to circumvent).

374. SCHNEIER, *supra* note 74, at 31.

375. Peter Pollack, *UK Wants Power to Demand Encryption Keys*, ARS TECHNICA, May 18, 2006 http://arstechnica.com/news.ars/post/20060518-6870.html.

376. Fisher, *supra* note 202.

377. Regulation of Investigatory Powers Act, 2000, ch. 23, §§ 17-18 (United Kingdom).

378. Fisher, *supra* note 202.

379. *Id.*

380. Pollack, *supra* note 375.

381. *See* Regulation of Investigatory Powers Act §§ 17-18, 49; *see also* Communications Assistance for Law Enforcement Act, 47 U.S.C. §§ 1001-10 (2006).

382. Regulation of Investigatory Powers Act §§17-18.

383. *Id.* § 49.

384. *See* Communications Assistance for Law Enforcement Act §§ 1001-10.

communications.[385] Just as back door wiretap and interception capabilities may be exploited by hackers or those inside law enforcement agencies, so too would the ability to request encryption/decryption keys.[386]

VII. GREASING THE SLIPPERY SLOPE OF TECHNOLOGY IN SURVEILLANCE

Though balancing privacy and government security interests presents a daunting task to legislators and private citizens, some mistakenly view ubiquitous encryption as a potentially easy solution to the problem.[387] A recent article addressed the difficult balance between privacy and security with references to quantum computing, quantum encryption, and law enforcement alternatives to wiretapping, in a theorized landscape of pervasive encryption.[388] Although these references resonate with a certain technological sexual appeal, they may not, in reality, live up to their appearances.[389]

The article indicates that quantum computers will render current encryption schemes impotent.[390] Quantum computers, in theory, will be able to solve problems in minutes that conventional computers would take infeasible amounts of time to solve.[391] Regardless of the potential and theory, in reality, quantum computers maintain a place in research facilities solving trivial problems.[392] These machines employ complex and delicate equipment, and have yet to be produced in a commercially viable and scientifically accepted form.[393] Simply stated, most scientists in the field expect commercial quantum computers to reach the market in fifty years.[394]

The article also asserts that turn-key quantum encryption solutions have been released at a conference in 2005.[395] The quantum encryption referenced is

---

385. Pollack, *supra* note 375.

386. *Id.*

387. *See* Daniel J. Sherwinter, *Surveillance's Slippery Slope: Using Encryption to Recapture Privacy Rights*, 5 J. TELECOMM. & HIGH TECH. L. 501, 528-29. [hereinafter Sherwinter].

388. *Id.* at 516-18, 526-29.

389. *See e.g.* Marina Gorbis & David Pescovitz, *Bursting Tech Bubbles Before They Balloon*, IEEE SPECTRUM, Sept. 2006, at 55, *available at* http://www.spectrum.ieee.org/sep06/4435; R. Colin Johnson, *Quantum Encryption Secures High-Speed Data Stream*, E.E. TIMES, Nov. 07, 2002, http://www.commsdesign.com/news/tech_beat/OEG20021107S0031[hereinafter *Quantum Encryption Secures*].

390. Sherwinter, *supra* note 387, at 517-19.

391. Jason Pontin, *Q&A: D-Wave's Geordie Rose*, TECHNOLOGY REVIEW, Apr. 6, 2007, at 1, *available at* http://www.technologyreview.com/Infotech/18495/page1/?a=f. [hereinafter Pontin].

392. *Id.*

393. *Id.*

394. Gorbis & Pescovitz, *supra* note 389, at 50.

395. Sherwinter, *supra* note 387, at 518.

a key distribution system requiring optical networks.[396] Though an attractive prospect, quantum cryptography has its share of problems.[397] Quantum cryptography currently operates as a key distribution system, not a means to encrypt the content of an entire message.[398] This means that quantum cryptography must be used in conjunction with classical cryptography in order to create cipher text.[399] Though the encryption key may be transferred quickly and securely enough to be unbreakable, the message is still subject to the deficiencies of the classical encryption.[400] Another problem of quantum encryption is that it provides no protection against man-in-the-middle attacks, a common form of attack.[401] Vulnerability to man-in-the-middle attacks means essentially that, although quantum encryption is safe from passive eavesdropping, an active eavesdropper may impersonate the parties to the communication and gain access to the contents as it passes through his system.[402] Finally, the last problem with quantum encryption is the required fiber optic network.[403] Although companies are working on the problem, currently, quantum cryptography systems use dedicated fiber optic lines instead of the active fiber optic network.[404] The cost associated with running cryptographic systems on dedicated lines is prohibitive for almost any consumer.[405] Unless the problems and costs associated with

396. R. Colin Johnson, *Quantum Encryption Enters Product Phase*, E.E. Times, Apr. 28, 2005, at 44. [hereinafter R. Colin Johnson] (explaining that Quantum encryption systems require optic networks because they employ particles of light in differing energy states to replace ones and zeroes in typical encryption systems.) Nicolas Gisin, et. al, *Quantum Cryptography* 74 REVIEWS OF MODERN PHYSICS 145,149-152 (2002), *available at* http://astro.swarthmore.edu/comps/Gisin_quantum_crypto.pdf. [hereinafter Gisin].

397. Alex Salkever, *A Quantum Leap in Cryptography*, BUSINESS WEEK, July 15, 2003, http://www.businessweek.com/technology/content/jul2003/tc20030715_5818_tc047.htm; *see also* Gisin, *supra* note 396, at 12-20.

398. R. Colin Johnson, *supra* note 396, at 44.

399. *Id.*

400. *See Quantum Encryption Secures High-Speed Data Stream*, *supra* note 389. This quantum encryption scheme weakness means that if the classical encryption method that encodes the message can be broken in a matter of hours, no matter how secure the key transfer, the message is still vulnerable. *Id.*

401. *See* James Ford, Quantum Cryptography Tutorial (1996), http://www.cs.dartmouth.edu/~jford/crypto.html#2.

402. Bruce Schneier, *Hold the Photons!*, WIRED.COM, Dec. 15, 2005, http://www.wired.com/politics/security/commentary/securitymatters/2005/12/69841.

403. Brad Grimes, *Taking Aim at Distance, Cost of Quantum Crypto*, GOVERNMENT COMPUTER NEWS, Mar. 20, 2006, http://www.gcn.com/print/25_6/40120-1.html?topic=tech-report.

404. *Id.*

405. *See id.*

quantum cryptography can be properly addressed, it is unlikely these systems will be available for widespread use in the near future.[406]

Even though law enforcement agents are not hindered by quantum encryption, ubiquitous encryption could force them to use alternatives to wiretapping in order to find evidence.[407] Although encryption may force their use, these alternatives may not effectively garner call content information from VoIP communications.[408] Sherwinter's paper references the technique of monitoring electromagnetic signals broadcast from a computer's monitor.[409] This method of surveillance is called Van Eck Phreaking.[410] Van Eck Phreaking allows a person to view the information displayed on another's screen from a distance, even through walls.[411] As intriguing as this electromagnetic surveillance may be, this technique cannot circumvent VoIP encryption or gather call content information because conversations do not appear on the screen.[412] Additional options that may actually circumvent encryption, like spyware and Trojans, have unique limitations that may negate their effectiveness.[413] Employing spyware as an alternative to wiretapping requires not only the participation of government agencies but also from operating system and anti-spyware software companies, and may open new vulnerabilities within systems and communications.[414] Most of the wiretapping alternatives that offer the contents of communications require physical or logical access to the computer[415]

---

406. *Id.*

407. Bert-Jaap Koops, *The Crypto* Controversy*: A Key Conflict in the Information Society*, KLUWER LAW INTERNATIONAL, 1, 207 (1999), *available at* http://rechten.uvt.nl/koops/THESIS/thesis.htm. [hereinafter Koops].

408. *See id.* at 207.

409. Sherwinter, *supra* note 387, at 529.

410. Posting of Jonathan Grover, About Van Eck Phreaking, http://the.jhu.edu/upe/2004/03/23/about-van-eck-phreaking/ (Mar. 23, 2004)(on file with author).

411. *Id.*

412. Posting of Russell Shaw, "They" Can Spy on Your IM and VoIP Conversations – Through Walls!, http://blogs.zdnet.com/ip-telephony/?p=1553 (Apr. 20, 2007, 23:00)(on file with author) (explaining that essentially although IM messages appear on the computer screen, VoIP conversations are similar to a telephone call, the conversation is oral and never appears on the screen, therefore Van Eck Phreaking is ineffective in terms eavesdropping on these calls).

413. *See* Posting of Tim Lee, German Proposal Gives a New Perspective on 'Spyware', http://www.techdirt.com/articles/20071126/174251.shtml (Nov. 27, 2007, 17:10)(on file with author).

414. *Id.*

415. *See e.g. id*; Koops, *supra* note 407, at 207; Michael Le May & Jack Tan, *Acoustic Surveillance of Physically Unmodified PCs*, at 1-3, (Las Vegas, NV, June 26-29, 2006)(Proceedings of the 2006 International Conference on Security & Management, SAM 2006)(copy of paper on file with the *Tulsa Journal of Comparative & International Law*).

which exposes law enforcement agents to increased probability of detection, thereby decreasing their viability as alternatives to wiretapping.[416]

VIII. CONCLUSION

The fundamental differences between RIPA and CALEA highlight the difference between the United Kingdom and the United States and their respective commitments to privacy and government intervention.[417] The English requirement that a wiretap be signed only by a designated law enforcement official gives broader latitude to communication interceptions in the United Kingdom.[418] United States law enforcement communication interceptions require narrow judicial approval and greater specificity than their British counterparts.[419] These requirements were recognized by FBI director Louis J. Freeh as statutory protections where "Congress fashioned a comprehensive electronic surveillance framework that carefully balanced the communications security needs and privacy rights of individuals with the needs of law enforcement to fulfill its duty to protect the public and enforce the law."[420]

Even though CALEA extended the Omnibus Crime Control and Safe Streets Act, there is danger in the extension much past its current state.[421] As it stands, members of the FCC understand that CALEA needs change and tailoring to better fit the changing technologies without infringing on the rights of citizens.[422] There is a need for Congressional clarification of the reach of CALEA;[423] however, there is also a need for caution in that extension and clarification.[424] Though the FCC engaged in, and will continue to engage in, employing its ancillary jurisdiction under Title I,[425] the debate between the

---

416. *See* DIFFIE & LANDAU, *supra* note 42, at 295-99.

417. *Compare* Communications Assistance for Law Enforcement Act § 1002, *and* Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C.§ 2511 (2006), *with* Regulation of Investigatory Powers Act Part II § 32.

418. Regulation of Investigatory Powers Act. § 32.

419. *Compare* Omnibus Crime Control and Safe Streets Act of 1968 § 2511, and Foreign Intelligence Surveillance Act, 50 U.S.C. §1802, *and* Communications Assistance for Law Enforcement Act 47 U.S.C. §§ 1002, *with* Regulation of Investigatory Powers Act Part II § 32.

420. Freeh, *supra* note 28, at 3 (referring to the Omnibus Crime Control and Safe Streets Act of 1968
§§ 2510-2521).

421. FCC REPORT, *supra* note 220, at 55.

422. *See id.* at 54.

423. *Id.*

424. *Id.* at 55.

425. *Id.* at 56.

government's right to intercept communications and the right of privacy is growing increasingly heated.[426] The extension of CALEA and the RIPA encryption sections resemble laws passed by legislators that fail to understand the technology being regulated.[427] Though law enforcement needs tools such as wiretapping to perform their jobs, the leniency of regulations[428] allows these tools to be misused.[429] It is the misuse of proper law enforcement techniques and the Machiavellian national interest that could pave a path between the current incarnation of CALEA and an Orwellian future in the vein of 1984 where the government has "the power to keep its citizens under constant surveillance."[430]

426. Gohring, *supra* note 201.

427. Pollack, *supra* note 375.

428. FCC REPORT, *supra* note 220.

429. Pollack, *supra* note 375.

430. GEORGE ORWELL, 1984 335 (Oxford University Press 1984) (1949).