Federal Communications Law Journal

Volume 55 | Issue 2 Article 7

3-2003

Encryption Regulation in the Wake of September 11, 2001: Must We Protect National Security at the Expense of the Economy?

Matthew Parker Voors
Indiana University School of Law

NOTE

Encryption Regulation in the Wake of September 11, 2001: Must We Protect National Security at the Expense of the Economy?

Matthew Parker Voors*

* J.D. candidate, 2003, Indiana University School of Law—Bloomington. I would like to thank my family and friends for their love and support. Special thanks to Teresa Melton, without whom this Note would not have been possible. I would also like to dedicate this Note to my father, who recently passed away. Although he is no longer with me, his words of strength and encouragement always will be.

I. INTRODUCTION

> "This is our greatest fear, that, one day, a terrorist attack will succeed because law enforcement could not gain immediate access to the plaintext of an encrypted message . . . ."[1]

The Federal Bureau of Investigation ("FBI") identified Zacarias Moussaoui as a possible "last-minute" substitute and likely the twentieth hijacker in the September 11 atrocity.[2] After training at one of Osama bin Laden's terrorist camps in Afghanistan, Moussaoui moved to London a year before the attack. Ramzi Bin al-Shibh, an al Qaeda member, flew to London immediately before Moussaoui left for his mission.[3] Al-Shibh, who roomed in Germany with Mohamed Atta, the mastermind of the September 11 attacks, tried to obtain an American visa four times between May and October but was denied each time.[4] Needing a replacement, al-Shibh is thought to have briefed his close friend, Moussaoui, of the situation. Moussaoui is believed to have then traveled to the United States in al-Shibh's place.[5] Once in the United States, Moussaoui deposited $32,000 in cash into a new bank account and began taking flying lessons in Norman, Oklahoma.[6] Later, Moussaoui received $14,000 from al-Shibh who also had wired money to Marwan al-Shehhi,[7] Atta's nephew and the terrorist

1. Charles Barry Smith, *Current U.S. Encryption Regulations: A Federal Law Enforcement Perspective*, 3 N.Y.U. J. LEGIS. & PUB. POL'Y 11, 16 (2000).

2. Chitra Ragavan, *The Case of a '20th Hijacker'?*, U.S. NEWS & WORLD REP., Dec. 24, 2001, at 20.

3. *Id*.

4. *Id*.

5. *Id.*

6. *Id*.

7. *Id*.

who piloted United Airlines Flight 175 into the South Tower of the World Trade Center.[8]

Given all this, it was not until Moussaoui moved to Minneapolis, Minnesota, that warning bells started to ring. Moussaoui enrolled at the Pan Am International Flight Academy in Minneapolis to be trained in flying the bigger jumbo jets,[9] specifically 747s.[10] While training on simulators at the flight school, he informed his instructors that "[h]e wanted to concentrate only on the midair turns, not the takeoffs and landings."[11] The flight school notified the FBI about this suspicious behavior, and that agency later arrested Moussaoui for remaining in the United States on an expired visa.[12]

Although the FBI arrested Moussaoui, who otherwise might have been a pilot in the September 11 attacks, authorities failed to detect the other terrorists. The U.S. authorities failed to discover Mohamed Atta, Waleed al-Shehri, Wail al-Shehri, Abdulaziz al-Omari, and Satam al-Suqami, who flew American Airlines Flight 11 into the North Tower of the World Trade Center.[13] Similarly, they failed to detect Ahmed al-Ghamdi, Marwan al-Shehhi, Fayez Ahmed, Mohald al-Shehri, and Hamza al-Ghamdi, who hijacked and aimed United Airlines Flight 175 into the South Tower of the World Trade Center.[14] Authorities never discovered terrorists Khalid al-Mihdhar, Nawaq al-Hamzi, Hani Hanjour, Salem al-Hamzi, and Majed Moqed, who directed American Airlines Flight 77 into the Pentagon,[15] or Saeed al-Ghamdi, Ziad al-Jarrah, Ahmed al-Nami, and Ahmed al-Haznawi, who commandeered United Airlines Flight 93 that crashed in Pennsylvania, but allegedly attempted to hit the White House.[16]

In the wake of the September 11 attacks, many Americans are asking the same question: How could U.S. authorities and intelligence agencies fail to detect the September 11 plot? With the exception of a few of the terrorists, they were young and needed direction.[17] They needed money to carry out their missions and, most importantly, they needed intelligence to help plan and coordinate that fateful day. Where were the communications

8. *Search for the Missing Pieces*, SUNDAY TIMES (LONDON), Sept. 23, 2001, at Features.

9. Susan Headden et al., *The Banality of Evil*, U.S. NEWS & WORLD REP., Oct. 1, 2001, at 25-26.

10. Evan Thomas et al., *The Road to September 11*, NEWSWEEK, Oct. 1, 2001, at 38.

11. *Id.*

12. *Id.*

13. *Search for the Missing Pieces*, *supra* note 8.

14. *Id.*

15. *Id.*

16. *Id.*

17. *See id.*

between the leaders in Afghanistan and the terrorists here in the United States? Where were the communications that would have signaled the intelligence agencies that an attack on the United States was imminent? Even now, a year and a half after the attack, the question of how the terrorists communicated remains a mystery.[18]

Newspapers and magazines quickly pointed the finger, but many could not conclude who was to blame.[19] They have, however, noticed one common thread that runs through many of the FBI reports from both before and after the terrorist attacks on September 11—the Internet played a key role in planning the terrorist attacks.[20]

This Note argues that although privacy and economic concerns have ruled the encryption debate during the past decade, the move toward increased privacy on the Internet and relaxed encryption regulation, designed to promote electronic commerce ("e-commerce"), comes at the expense of national security and the protection of Americans' safety. Part II of this Note provides background on encryption. In particular, Part II explains encryption and details its use throughout history. Additionally, Part II examines how businesses use encryption to secure their communications and financial transactions on the Internet. This Section also observes that this technology is employed by terrorist organizations to accomplish the same goal: to send private communications. Part III details the history of encryption regulation during the last decade and addresses why the government has relaxed its stance even though encryption ultimately poses such a threat. Part IV analyzes whether encryption regulation will provide the intelligence community the tools to deal with terrorists who are now technologically savvy, or whether regulation will hurt the nation's already wounded economy. Part V examines Magic Lantern, cutting-edge technology developed by the FBI that effectively incorporates the privacy benefits of encryption while still providing Americans protection in this new era of terrorism. More specifically, Part V will argue this new technology should be implemented because it balances privacy and economic concerns with national security needs. Finally, Part VI will conclude by proposing the adoption of the FBI's new technology as a way to protect privacy and economic concerns while ensuring national security.

18. *See generally* Kevin Whitelaw, *Unanswered Questions: There Are Still Big Gaps in What Is Known About the 9/11 Plotters*, U.S. NEWS & WORLD REP., Sept. 9, 2002, at 28.

19. *See generally Search for the Missing Pieces*, *supra* note 8.

20. *See* Associated Press, *Attacks Renew Encryption Debate* (Sept. 24, 2001).

II. HISTORY OF ENCRYPTION

> "If all the personal computers in the world—260 million computers—were put to work on a single [strongly encrypted] message, it would still take an estimated 12 million times the age of the universe . . . to break a single message . . . ."[21]

A. What Is Encryption?

Encryption is a technique that changes a plaintext message from its original form by replacing or rearranging the letters and numbers and converting the message into an indecipherable form using a mathematical algorithm and a key.[22] The length of the encryption key is measured in bits and determines the strength of the encryption program.[23] For example, an encryption key that is 40 bits in length yields 1 billion possible keys or combinations, a key with 56 bits has 72 trillion, and a key that measures 128 bits produces a gazillion solutions.[24]

There are two types of encryption systems: private-key and public-key.[25] Encryption systems began with private-key systems that use algorithms and a symmetric key to encrypt and decrypt messages.[26] Private-keys are less private because they run into a fundamental problem. Since "the same key is used to both encrypt and decrypt the message," the key must be e-mailed to the receiver in order for the message to be decrypted and read.[27] Private-key encryption systems offer limited security because encrypted messages can be read if a third party intercepts the key when it is transmitted from the sender to the receiver.[28] This flaw thwarted early efforts for businesses and the public to use encryption effectively and safely.[29]

---

21. *Security and Freedom Through Encryption (SAFE) Act: Hearing on H.R. 695 Before the Subcomm. on Courts and Intellectual Property*, 105th Cong. 45 (1997) (statement of William P. Crowell, Deputy Director, National Security Agency).

22. J. Terrence Stender, Note, *Too Many Secrets: Challenges to the Control of Strong Crypto and the National Security Perspective*, 30 CASE W. RES. J. INT'L L. 287, 294-95 (Winter 1998); *see also* Kurt M. Saunders, *The Regulation of Internet Encryption Technologies: Separating the Wheat from the Chaff*, 17 J. MARSHALL J. COMPUTER & INFO. L. 945, 947-48 (Spring 1999).

23. Marc S. Friedman, *Some Observations on Encryption—Plain*, *Simple*, *and Unencrypted*, 3 N.Y.U. J. LEGIS. & PUB. POL'Y 5, 8 (2000).

24. *Id*.

25. Tricia E. Black, Note, *Taking Account of the World An It Will Be: The Shifting Course of U.S. Encryption Policy*, 53 FED. COMM. L.J. 289, 296 (2001).

26. *See* Stender, *supra* note 22, at 295.

27. Black, *supra* note 25, at 296.

28. *Id.*; *see also* Stender, *supra* note 22, at 295.

29. *See* Stender, *supra* note 22, at 295-96.

The invention of public-key encryption in the mid-1970s solved the weakness of private-key systems.[30] Public-key encryption systems require two asymmetrical keys: one used by the sender to encrypt (called a public-key) and another used by the receiver to decrypt (called a private-key).[31] Although these keys are a matched set and "mathematically related," it is impossible to decrypt the message by accessing only the public-key because the private-key decrypts the message.[32] Thus, the receiver publishes his public-key so that the sender may use it to encrypt the message he wishes to send to the receiver.[33] The second key, the private-key, is held only by the receiver, who keeps it private so that only he may decrypt the message.[34] Therefore, the sender looks up the receiver's published public-key, encrypts the message utilizing the receiver's public-key, and then sends the message to the receiver.[35] The receiver then decrypts the message by using his private-key, which only he can access.[36] If the receiver wants to respond to the sender, he would complete the same process in reverse.

Once a message is encrypted, it can be read one of two ways. First, as mentioned above, the receiver can use a private-key to access and decrypt the message. The second method, a "Brute Force Attack," is far more complex and occurs when a computer program attempts to use all possible keys to crack the encryption code.[37] In layman's terms, this is the equivalent of a man holding a key ring with millions of keys, trying each key in the lock until he finds one that matches. This process devours massive amounts of computer power and takes an inordinate amount of time.[38]

30. *Id*. at 296.

31. *Id*. at 295.

32. *See id*. at 296.

33. *Id*.

34. *Id*.

35. Black, *supra* note 25, at 296.

36. *Id*.

37. Andres Rueda, *The Implications of Strong Encryption Technology on Money Laundering*, 12 ALB. L.J. SCI. & TECH. 1 (2001); Stender, *supra* note 22, at 287; Bernadette Barnard, *Leveraging Worldwide Encryption Standards Via U.S. Export Controls: The U.S. Government's Authority to "Safeguard" The Global Information Infrastructure*, 1997 COLUM. BUS. L. REV. 429, 435.

38. Interview by Russell D. Hoffman with Phil Zimmerman, Author of PGP, WALE Radio (Feb. 2, 1996), *available at* http://animatedsoftware.com/hightech/philspgp.htm.

B. Background on Encryption

Although encryption may appear to be a modern phenomenon, it can be traced back to 1900 B.C.[39] Governments and militaries used cryptography to keep their secrets safe.[40] One of the earliest forms of cryptography was developed and used by Julius Caesar to send his military orders safely.[41] The aptly named Caesar Cipher is a simple substitution cipher and employs the use of two alphabets, one directly written above the other.[42] The bottom alphabet is moved to the right (or left) of the top alphabet.[43] The bottom letters then represent the letters in the top alphabet.[44] For example, if the bottom alphabet was shifted one letter to the right an A would represent a B, a B would represent a C, and so on. Thus, using this cipher text, the word PLANE would be enciphered QMBOF. This message would be kept secret because only the sender and the recipient of the message would know how to rearrange the letters to convert the cipher text into plaintext. In addition, changing the code at regular intervals can enhance the security of the messages.[45]

Since that time, cryptography has become more complex.[46] During World War I and World War II, encryption played an integral role and helped secure victories for the United States.[47] For example, in World War II the "Purple" codes used by the Japanese and the "Ultra" codes used by the Germans were thought to be "unbreakable."[48] The United States' efforts and advancements in cryptography helped crack the codes and were vital in winning the war.[49]

39. History: The Origins of Encryption, *available at* http://www.biz.uiowa.edu/class/6k180_park/Student-Reports/rnation/History.htm.

40. Stender, *supra* note 22, at 289.

41. *See* Adam C. Bonin, *Protecting Protection: First and Fifth Amendment Challenges to Cryptography Regulation*, 1996 U. CHI. LEGAL F. 495, 497 (1996).

42. Daniel Olson, *Analysis of Criminal Codes and Ciphers*, 2 FORENSIC SCI. COMM., (2000), *available at* http://www.fbi.gov/hq/lab/fsc/backissu/jan2000/olson.htm.

43. *Id*.

44. *Id*.

45. *See id*.

46. *See generally* History: The Origins of Encryption, *supra* note 39; *see also* Black, *supra* note 25, at 294.

47. *See* Stender, *supra* note 22, at 300; *see also* Joel C. Mandelman, *Lest We Walk into the Well: Guarding the Keys–Encrypting the Constitution: To Speak, Search, and Seize in Cyberspace*, 8 ALB. L.J. SCI. & TECH. 227, 230 (1998).

48. Mandelman, *supra* note 47, at 230; *see also* Olson, *supra* note 42; Stender, *supra* note 22, at 300.

49. *See* Mandelman, *supra* note 47, at 230.

C. Recent Encryption Advancements

Recent advancements made encryption more available so its use was no longer limited to military and government.[50] In the mid-1970s, two scientists from Stanford University invented public-key encryption.[51] This advancement allowed messages to be encrypted, sent, and decrypted without e-mailing the sender's private-key.[52] As discussed *infra*, this eliminated the threat that the private-key might be intercepted and subsequently compromise the safety of later messages.[53]

In the early to mid-1980s, Phil Zimmerman developed software that implemented the concept of public-key encryption and revolutionized the world's perception of encryption.[54] Pretty Good Privacy ("PGP"), as the software is called, was released in the early 1990s.[55] The program extended the use of encryption from major governments and militaries to ordinary businesses and private citizens.[56]

Although PGP was a boon to many businesses and private individuals, the United States government did not agree. In fact, the government deemed encryption software vital to preserving national security.[57] The State Department classified it as a munition and listed it in the Arms Export Control Act with other military weapons such as machine guns, bombs, and missiles, thus prohibiting it from export without a license.[58] Aware of this, Zimmerman gave away PGP for free on the Internet.[59] The government, however, decided that providing PGP on the Internet constituted an export.[60] This decision prompted the U.S. government to conduct a three-year investigation of Zimmerman for violating the Arms Export Control Act.[61] After a lengthy investigation, however, Zimmerman was never prosecuted.[62]

50. *See* Stender, *supra* note 22, at 296.
51. *Id*.
52. *Id*.
53. *See supra* notes 30–36 and accompanying text.
54. Interview by Russell D. Hoffman with Phil Zimmerman, Author of PGP, WALE Radio (Feb. 2, 1996), *available at* http://animatedsoftware.com/hightech/philspgp.htm.
55. *Id*.
56. *See id.*
57. *Id.*
58. *Id.*
59. *See id.*
60. *See id*.
61. *Id.*
62. *See id*.

D. Use of Encryption by Business and the Service Industry

The use of encryption systems is no longer limited strictly to military use. Businesses, hospitals, utilities, and communications companies use encryption to protect their information from being compromised.[63] Increasingly, businesses are utilizing the Internet and incorporating their sales and marketing plans to include e-commerce.[64] In fact, experts predicted in 1998 that "[b]y 2002, the Internet may be used for more than $300 billion worth of commerce between businesses."[65] To effectively utilize e-commerce, businesses can guarantee the safety of their communications by using encryption.[66] Without such safety measures in place, customers who conduct financial transactions or make credit card purchases may fall prey to those who exploit such information.[67] For example, Amazon.com, one of the largest online retailers, uses encryption to secure customers' personal information and credit card numbers.[68] Similarly, Ameritrade, one of the largest online stock trading companies, uses encryption to ensure the security of its customers' stock trades.[69] Additionally, Web browsers, such as Internet Explorer and Netscape, use encryption to secure their users' credit card transactions.[70]

Hospitals also use encryption to ensure the privacy of patients' records.[71] In an effort to cut costs and increase access to information, hospitals began storing medical records in their computers, thus allowing

63. *See* Black, *supra* note 25, at 294; *see also* Mandelman, *supra* note 47, at 236-37; Saunders, *supra* note 22, at 945.

64. *See generally* Lynn Margherio et al., U.S. DEPARTMENT OF COMMERCE, THE EMERGING DIGITAL ECONOMY (1998), *available at* http://www.esa.doc.gov/508/esa/TheEmergingDigitalEconomy.htm.

65. *Id*.

66. *See* Black, *supra* note 25, at 294.

67. *See id*.

68. Amazon.com, Credit Card Security, *at* http://www.amazon.com/exec/obidos/tg/browse/-/468494/ref=hp_hp_ct_4_3/103-5728187-0035819:

> The Amazon.com Safe Shopping Guarantee protects you while you shop at Amazon.com, so that you never have to worry about credit card safety. Period. . . . It encrypts all of your personal information, including credit card number, name, and address, so that it cannot be read as the information travels over the Internet.

Id.

69. Ameritrade.com Security Statement, *at* http://www.ameritrade.com/tell_me_more/ (last visited Oct. 5, 2002): "It is the policy of the Ameritrade Secure Trading System to encrypt the transmission of all personal or financial Web-based information that is transmitted between our site and your browser." *Id*.

70. Carrie Kirby, *New Encryption Laws for E-mail Unlikely*, S.F. CHRON., Oct. 6, 2001, at B1, *available at* 2001 WL 3416304.

71. *See* Paul Korzeniowski, *VPNs Become Key Part of Enterprise Networks*; *Technology Information*, BUS. COMM. REV., Mar. 2000, at 28.

them to be accessed by patients, doctors, and other health care personnel.[72] St. Vincent Hospital, in Birmingham, Alabama, for example, recently upgraded its encryption from 40 bits to 128 bits to ensure the privacy of its patients' medical records.[73] Others in the medical field have followed suit. For example, a medical practice in Palo Alto, California, electronically stores patients' medical records to give medical personnel easier access to the records and to improve communication between doctors and nurses.[74]

E. Use of Encryption by Terrorist Organizations

Although encryption is necessary for businesses' success on the Internet, it is also becoming a sinister tool for terrorist organizations to keep their plans and communications secret.[75] The FBI's success in detecting and preventing terrorist activities depends largely on its ability to gather this type of intelligence.[76] Thus, in the words of Louis Freeh, former Director of the FBI: "[U]nbreakable encryption ultimately will devastate our ability to fight crime and prevent terrorism. . . . [and] will allow drug lords, spies, terrorists and even violent gangs to communicate . . . with impunity."[77] Experts and the public as a whole are beginning to realize that new technology revolutionizes legitimate businesses as well as terrorist organizations. "The new terrorism is of a different genre. . . . It does not consist of guerillas sheltering in the countryside making occasional incursions into the cities, but. . . . makes use of air travel and the Internet. It uses similar encryption algorithms to hide its internal communications."[78]

The FBI estimates that more than 1,000 foreign nationals with suspected terrorist ties currently live in the United States.[79] Previous attacks

72. *See id*.

73. *Id*. at 32.

74. Rick Whiting, *Patient-Privacy Issue Gets a Doctor's Care*, INFORMATIONWEEK, Dec. 24, 2001, at 40.

75. *Threat of Terrorism to the United States: Statement before the U.S. Senate Comms. on Appropriations*, *Armed Servs.*, *and Select Comm. on Intelligence*, 107th Cong. (2001) [hereinafter *Threat of Terrorism to the United States*] (statement of Louis J. Freeh, Director, FBI), *available at* http://www.fbi.gov/congress/congress01/freeh051001.htm.

76. *Counterterrorism and Infrastructure Protection: Hearing Before a Subcomm. of the Senate Comm. on Appropriations*, 106th Cong. 45 (1999) (statement of Louis J. Freeh, Director, FBI).

77. *The Impact of Encryption on Public Safety and Law Enforcement*, *Focusing on the Security Needs of Business and Industry and the Use of Encryption by Organized Crime and Terrorists: Hearing before the Senate Subcomm. on Tech*., *Terrorism*, *and Gov't Info*., *Senate Comm. on Judiciary*, 105th Cong. 43 (1997) (statement of Louis J. Freeh, Director, FBI).

78. George Yeo, *S'pore a Free Port but it Will Give No Quarter to Terrorism*, THE STRAITS TIMES (SINGAPORE), Oct. 12, 2001, at 26, *available at* LEXIS News Library.

79. Thomas et al., *supra* note 10, at 38.

by Osama bin Laden's al Qaeda organization indicate that sleeper cells, consisting of a number of al Qaeda followers, journey to the target country to live until they are told when, where, and how to carry out their attacks.[80] The terrorists responsible for the attack on the United States lived among us for a year[81] performing everyday activities including doing laundry, working out, eating pizza, and shopping at local malls and grocery stores.[82] One neighbor described them as "five good guys,"[83] and others believed the terrorists were "students from the university."[84]

In between these times of normal behavior, the terrorists also planned for their upcoming attack. They enrolled in flight school and practiced their piloting skills, which would be needed when the time came.[85] They also bought box cutters that were used to take the planes by force.[86] In addition, the "tech-savvy hijackers . . . appeared to use a web of electronic connections to plan and communicate in relative anonymity."[87]

One source called bin Laden's group "the coming thing in the age of modern terrorism."[88] The head of the U.S. National Security Agency voiced his concern that al Qaeda's growing use of the Internet and encryption to hide communications has eluded even U.S. technology.[89] George Tenet, Director of the Central Intelligence Agency, told Congress recently that al Qaeda is "the nation's most immediate and serious transnational threat."[90] U.S. officials report that "encryption has become the everyday tool of Muslim extremists . . . . It's become so fundamental to the operations of these groups that bin Laden and other Muslim extremists are teaching it at their camps in Afghanistan and Sudan."[91] Bin Laden's terrorist organization has advanced and become more sophisticated. The organization relies on computers and advanced encryption techniques to

80. *Id*. at 40.

81. Edward T. Pound, *Under Seige*, U.S. NEWS & WORLD REP., Sept. 24, 2001, at 10.

82. Headden et al., *supra* note 9, at 23.

83. *Id*.

84. *Id*. at 24.

85. *Id*.

86. *Id*.

87. David Fallis and Ariana Eunjung Cha, *Agents Following Suspects' Lengthy Electronic Trail*; *Web of Connections Used to Plan Attack*, WASH. POST, Oct. 4, 2001, at A24.

88. Peter Grier, *A Terrorist Version of NATO?*, CHRISTIAN SCI. MONITOR, Feb. 16, 2001, at 1.

89. *Id.*

90. *Id.*

91. Jack Kelley, *Terror Groups Hide Behind Web Encryption*, USA TODAY, Feb. 15, 2001, *available at* http://www.usatoday.com/life/cyber/tech/2001-02-05-binladen.htm.

communicate through encrypted e-mail.[92] In addition, the al Qaeda network employs "top-notch software engineers."[93] This new technology makes it more difficult to gather intelligence and to expose bin Laden's plans of terror. Currently, bin Laden uses powerful encryption devices that are commercially available and increasingly easy to obtain.[94]

Although the FBI investigation has not yet found any direct evidence that encryption played a role in the September 11 attacks, there is conclusive evidence that terrorists, including those in bin Laden's al Qaeda network, used encryption to encode phone communications and e-mails.[95] The investigation of Ramzi Yousef, the terrorist who planned and directed the 1993 attacks on the World Trade Center, uncovered that Yousef used encryption in a plot to destroy eleven U.S. commercial airliners.[96] In 1998, Wadih El Hage, one of the terrorists suspected of bombing the U.S. embassies in east Africa, sent encrypted e-mails to members of al Qaeda before the bombings took place.[97] In 1999, Khalil Deek used encryption to plan bombings in Jordan.[98] More recently, "[s]even months [before the attacks on the World Trade Center and the Pentagon], a widely quoted newspaper report had claimed that bin Laden's followers were operating a communications network based on encrypted messages concealed inside pornographic pictures."[99]

Bin Laden's resume of terror also includes other attacks that evidence the use of encryption:

- February 26, 1993: World Trade Center bombed; 6 killed and more than 1,000 injured;[100]
- October 3, 1993: 18 American service men attacked and killed in Somalia;[101]

92. *Threat of Terrorism to the United States*, *supra* note 75; Bob MacDonald, *It's All or Nothing*; *No Half-Measures in Fight Against Terrorism*, TORONTO SUN, Oct. 9, 2001, at S5.

93. Kirby, *supra* note 70.

94. J. William Gurley, *From Wired to Wiretapped*: *Forget Privacy Rights. The Real Problem with Government Net Snooping Is That it Won't Work*, FORTUNE, Oct. 15, 2001, at 214.

95. John Rendleman, *Mixed Messages*, INFORMATIONWEEK, Oct. 1, 2001, at 18.

96. Kelley, *supra* note 91; *see* Alison Mitchell & Todd S. Purdum, *Ashcroft*, *Seeking Broad Powers*, *Says Congress Must Act Quickly*, N.Y. TIMES, Oct. 1, 2001, at A1.

97. Kelley, *supra* note 91.

98. *Id*.

99. Duncan Campbell, *Online*: *How the Plotters Slipped U.S. Net*: *Spy Networks Failed to Detect Email and Satellite Conversations Used to Plot the Attack on the U.S.—and Now America Wants to Know What Went Wrong*, THE GUARDIAN (LONDON), Sept. 27, 2001, at 1.

100. Peg Tyre, *An Icon Destroyed*, NEWSWEEK, Sept. 11, 2001, *at* http://www.msnbc.com/news/627092.asp.

101. *Id.* at 21.

- August 7, 1998: U.S. embassies bombed in Africa, 301 killed and 5000 injured;[102]
- October 12, 2000: U.S.S. Cole attacked while in Yemen, 17 killed, 39 injured;[103]
- September 11, 2001: World Trade Center and Pentagon attacked, thousands killed and injured.[104]

Although the reports only *allege* encryption was used to plan September 11, hard evidence proves the terrorists used the Internet to plan their attacks.[105] "FBI assistant director Ron Dick, head of the US National Infrastructure Protection Centre, told reporters that the hijackers had used the net, and 'used it well.'"[106] In one instance, two of the hijackers equipped with laptops would not check into a Hollywood, Florida, hotel unless they had around-the-clock Internet access in their room.[107] When the terrorists learned that such access was not available, they became angry and left.[108] The terrorists also used the Internet to purchase "at least nine of their [airline] tickets for the four doomed September 11 flights."[109] The terrorists frequently used computers at public libraries to access the Internet[110] and used the Web to steal social security numbers and obtain fake drivers' licenses.[111]

III. ENCRYPTION REGULATION OVER THE LAST DECADE

The regulation of encryption has been a compromise between protecting our national security by restricting access to encryption used abroad, and recognizing businesses' legitimate need for this technology overseas. Early in our history, the U.S. government realized the important role that encryption could play in keeping military communications secret.[112] To keep this technology firmly in American hands, the government worked to place restrictions on encryption both domestically and abroad.[113]

102. *Id.*
103. *Id.*
104. *Id.* at 20.
105. *See generally* Campbell, *supra* note 99.
106. *Id*.
107. Fallis & Cha, *supra* note 87, at A24.
108. *Id.*
109. *Id.*
110. *Id.*
111. Headden et al., *supra* note 9, at 26.
112. Stender, *supra* note 22, at 289.
113. *See* Black, *supra* note 25, at 298; *see also* Stender, *supra* note 22, at 300.

A. The Struggle Between National Security and an Evolving Global Economy

As the U.S. economy evolved and expanded overseas, it became apparent that the use of encryption technology proved as vital to business as it was to the military.[114] As evidence of this, the government classified encryption as a "dual-use" technology, meaning it had both military and civilian use.[115] This opened the door for businesses and average citizens to use encryption to keep their information secret.[116] The government, however, restricted the types of encryption programs used overseas.[117]

The government's policy, aimed at protecting national security, came at the expense of our nation's economy. Export regulations mandated that encryption software sent abroad possess limited key length, thus diminishing the strength of the program.[118] Businesses that demanded stronger encryption programs to protect their information had to submit to a governmental review to obtain a license to export higher-strength encryption programs.[119] This policy left overseas American businesses with the choice of using less than full strength software to protect their information or subjecting themselves to a protracted governmental review process. In addition, export restrictions left software companies that produced encryption programs unable to compete with foreign software companies that did not have to comply with the stringent U.S. regulations.[120]

B. Regulation of Encryption Through Export Restrictions

Before 1996, the State Department restricted the export of encryption programs through the Arms Export Control Act, the Export Administration Regulations ("EAR"), and the International Traffic in Arms Regulation ("ITAR").[121] EAR allowed the export of products using only a general license.[122] The government's classification of encryption software as a munition, however, subjected it to tighter export regulations.[123] Under ITAR, a seller of encryption software needed separate licenses before

114. Black, *supra* note 25, at 299.
115. *Id*.
116. *See id*.
117. *Id.* at 297.
118. *Id.*
119. *See id.*
120. *See id.*
121. *Id.* at 298; Stender, *supra* note 22, at 302.
122. Stender, *supra* note 22, at 303.
123. *See* Black, *supra* note 25, at 298.

exporting a munition. The applications for licenses required approval of the Defense Department and the National Security Agency.[124]

On November 15, 1996, President Clinton issued an Executive Order transferring the regulation of "dual-use" encryption from the State Department to the Department of Commerce.[125] This transfer of power allowed the Department of Commerce to control the exportation of all encryption technology that was not developed or used strictly for military purposes.[126] The shift of power from the Department of Defense to the Department of Commerce benefited businesses that used or made encryption software.[127] This significantly decreased the amount of time exporters waited for licenses to ship encryption products overseas.[128] On January 12, 2000, the Clinton administration continued to eradicate export restrictions on encryption technology with the announcement that virtually all types of encryption programs could be exported without restriction.[129] The final blow to export restriction came in July 2000, with the announcement that all U.S. companies could export, without a license, any encryption products "to any end-user" in selected countries.[130]

C. Attempts to Regulate Encryption Domestically

Although the United States primarily focused on the regulation of encryption through export restrictions, its efforts briefly extended to domestic regulation. In 1993, the Clinton administration implemented the "Clipper Chip" initiative.[131] Its purpose was to combat terrorists, drug traffickers, and spies who used encryption to elude law enforcement.[132] The government planned to accomplish this bold goal by mandating that encryption technology be subject to a mandatory "key escrow" program.[133] The plan for the key escrow system required that a copy of the decryption keys be held for safekeeping by a Trusted Third Party ("TTP").[134] The Clipper Chip initiative was designed to allow businesses to use stronger

124. Stender, *supra* note 22, at 303.
125. Black, *supra* note 25, at 299.
126. *Id*.
127. *See id*.
128. *Id*.
129. *Id.*
130. *Id.*
131. *Id*. at 300.
132. Saunders, *supra* note 22, at 950.
133. *Id*. at 951.
134. Black, *supra* note 25, at 301.

encryption systems, while ensuring that law enforcement could access the keys should the need arise.[135]

Despite the government's efforts to implement the Clipper Chip initiative, the program ultimately failed. Many viewed the key escrow system as one that would create an inferior product because it would not grant the protection businesses demanded from the encryption software.[136] The software industry, as well as the business community, argued that mandating encryption software be accessible by a third party created a "back door" through which one could access protected information.[137] Businesses at home and abroad feared the government would abuse its power to access the back door, thus obtaining confidential information "under the guise of law enforcement and national security."[138] The Clinton administration, unable to address these concerns and to satisfy those in the computer and business industries, eventually abandoned the Clipper Chip initiative.[139]

IV. THE EFFECT OF ENCRYPTION REGULATIONS: WOULD REGULATIONS STOP TERRORISM OR HURT THE ECONOMY?

> "Unfortunately, every time the United States has a lasting peace, it becomes complacent about security and overly focused on economic growth. History, however, has repeatedly admonished the United States that such a mistake may have mortal ramifications."[140]

With the terrorist attacks of September 11 fresh in our minds, many are compelled to ask one question: If encryption regulations had been in place, would the attacks still have occurred? In fact, two days after the terrorist attacks on the World Trade Center and the Pentagon, some in Congress did more than ask the question.[141] In a speech on the Senate floor, Senator Judd Gregg renewed the previous call for regulations on encryption products that had been resolved in recent years.[142] Few of his colleagues from either side of the aisle answered the Senator's call to arms. The reason for the silence in Congress was likely based on encryption's previous regulatory history.[143] Specifically, many thought the regulations would

135. Stender, *supra* note 22, at 308.

136. *See* Black, *supra* note 25, at 301.

137. *Id.*

138. *Id.*

139. Saunders, *supra* note 22, at 951.

140. Stender, *supra* note 22, at 336.

141. Declan McCullagh, *Congress Mulls Stiff Crypto Laws*, WIRED NEWS, Sept. 13, 2001, *at* http://www.wired.com/news/politics/0,1283,46816,00.html.

142. *Id.* Senator Gregg is a Republican senator from New Hampshire.

143. *See id.*

cripple business and compromise individual privacy rather than prevent terrorist attacks.[144]

Regulations that weakened the strength of encryption programs or that mandated back doors jeopardized security on the Internet and had major consequences on business as well as the economy. It is virtually undisputed that strong encryption is essential for providing security on the Internet. Faced with using altered encryption programs, businesses likely would be hesitant to use the technology because they would be unable to guarantee privacy for their customers. Without such security measures for those passing confidential information online, e-commerce and other industries dependent on encryption would suffer a crippling blow, dragging our economy with it. This move would not only weaken encryption for terrorists, but would also do the same to businesses and other industries as well.[145]

Even if the government passed legislation that required mandatory back doors so law enforcement could access suspicious encrypted e-mails, other encryption programs without back doors are readily available.[146] Programs such as PGP have been available online and are currently sold without back doors. In addition, terrorists would not use encryption programs if law enforcement held the keys and a back way into their communications.[147] Thus, even if previous regulations on encryption were revived, many terrorist groups would buy encryption programs in other countries without back doors to evade detection.[148]

More importantly, the investigation into the terrorist attacks on September 11 revealed that encryption *might* have played a role.[149] Evidence suggests that in addition to using encryption, bin Laden's organization also uses steganography.[150] Steganography is a technique that hides messages within pictures, music, and other media.[151] For example, after a plaintext message is encrypted, the message is hidden in a picture or MP3 file using a steganography software file.[152] The hidden and encrypted

144. *See id.*

145. Elinor Mills Abreu, *Opening Encryption 'Back Door' is Problematic*, *Experts Say*, (Sept. 26, 2001), *at* http://staging.infoworld.com/articles/hn/xml/01/09/26/010926hnbackdoor.xml?Template=/.

146. *Id*.

147. *Kirby*, *supra* note 70.

148. *See id.*

149. *See*, *e.g.*, Kevin Maney, *Osama's Messages Could Be Hiding in Plain Sight*, USA TODAY, Dec. 19, 2001, at B6.

150. *Id.*

151. *Id.*

152. *Id.*

message would then be placed on a Web page and could be pulled up at any time by others. This ingenious process would prevent intelligence agencies from detecting that encrypted messages were being sent, not to mention maximizing the security of the communications.

Thus, since previous regulations merely give the illusion of protection against terrorism while potentially crippling the American economy, a better solution must be ascertained. If restricting exportation, requiring licensing, or keeping key escrow accounts will not stop terrorists from secretly communicating through encrypted messages, then what will? Is there an option government regulators have yet to discuss? The answer lies in new FBI technology, that will allow the U.S. government to stare through the proverbial keyhole instead of using a brute force attack to kick down the door.

V. LEADING THE WAY WITH ITS MAGIC LANTERN: DOES NEW TECHNOLOGY DEVELOPED BY THE FEDERAL BUREAU OF INVESTIGATION SOLVE THE ENCRYPTION PROBLEM?

Finding a way to crack encryption has baffled law enforcement agencies. Historically, if the government discovered a suspicious e-mail that was encrypted and wanted to read it, it had two options—it could obtain the private-key from the sender, or it could attempt to break the code through a brute force attack.[153] The first option, requiring terrorists to supply the private-key, is not plausible because this would reveal the investigation to the terrorists. In addition, those under investigation would not want to incriminate themselves if they were engaged in illegal activity. The second option, cracking the code by a brute force attack, is possible, but the process involves a massive amount of computer power and an equally large number of staff hours.[154] Neither option is attractive. Furthermore, law enforcement's efforts may be for naught, since the encrypted message could just as easily be directions to meet for a basketball game as it could be instructions to carry out a terrorist attack. What if, however, a third option existed?

153. *See* Rueda, *supra* note 37, at 23.

154. Don E. Tomlinson, *Intellectual Property in the Digital Age: The Piracy/Counterfeiting Problem and Antipiracy and Anticounterfeiting Measures,* 8 CURRENTS INT'L TRADE L.J. 3, 11 (Summer 1999); *Kenneth P. Weinberg, Cryptography: Key Recovery Shaping Cyberspace (Pragmatism and Theory),* 5 J. INTELL. PROP. L. 667, 674 (Spring 1998).

A. What Is Magic Lantern and How Does It Work?

A new project developed by the FBI, code-named Magic Lantern, has the capability of using the suspect's own computer and unwittingly employs the suspect himself to provide law enforcement its own private encryption key.[155] More specifically, Magic Lantern uses an existing program that logs all of the user's keystrokes and places them in a memory application.[156] This application enables the FBI to obtain access to the suspect's encrypted information by logging the suspect's keystrokes as he enters his password. The application then sends the password to the FBI at a remote location.[157] In essence, Magic Lantern allows the FBI to record a suspect's keystrokes and steal his private encryption key.[158]

Originally, software companies developed keystroke-logging software for home use so parents could monitor their children's activities on the Internet.[159] Soon after, some employers installed the keystroke-logging software to monitor their employees' computer habits while at work.[160] After discovering that hackers used keystroke-logging software to steal users' passwords, the government realized how useful it could be to obtain criminals' private-keys.[161] Thus, the government developed Magic Lantern.

Keystroke-logging software has advanced in recent years. Early attempts required FBI agents to enter the suspect's home or office where the computer was located and place the device inside the keyboard.[162] Recently, however, the FBI has combined new technology with the keystroke-logging software to make it more versatile and effective.[163] Now, the FBI's Magic Lantern program merges the old idea of keystroke-logging with a Trojan Horse virus so that the information can be collected and transmitted without ever having to enter the suspect's home or

155. Robert Vamosi, *We Know What You're Typing . . . and So Does the FBI*, MSNBC.COM, Dec. 7, 2001, *at* http://www.msnbc.com/news/669010.asp.

156. *Id.*

157. Bob Sullivan, *FBI Software Cracks Encryption Wall: 'Magic Lantern' Part of a New 'Enhanced Carnivore Project*,' MSNBC.COM, Nov. 20, 2002, *available at* http://www.msnbc.com/news/660096.asp.

158. Steven Levy, *Technology: Grappling with the New Politics of Software*, NEWSWEEK, Dec. 31, 2001, at 96.

159. Vamosi, *supra* note 155.

160. *Id.*

161. *See id.*

162. Sullivan, *supra* note 157.

163. *Id.*

business.[164] The FBI can accomplish this task in one of two ways. The easiest of the two begins by sending e-mail to the suspect's e-mail account.[165] The message would likely resemble the junk e-mail we all receive[166] or could even be attached to a family member's e-mail.[167] Once the suspect opens the message, the Trojan Horse virus, attached to the message, installs itself onto the suspect's computer, and begins logging the suspect's keystrokes.[168] The second process involves law enforcement exploiting flaws in the operating system to enter the computer to install the program.[169] In either case, the program would then record the keystrokes of the suspect, including the password to his encryption program, and transmit the information to the FBI while the suspect is online,[170] possibly by e-mail.[171]

B. Magic Lantern Works: Case in Point

The federal government has successfully employed Magic Lantern and used the information to convict a prominent mobster. Upon locating the suspect, the FBI obtained a court order from a federal magistrate to install the program.[172] Using an older version of Magic Lantern, the FBI entered the office of New Jersey mobster Nicodemo Scarfo and planted keystroke loggers on all the office's computers.[173] By recording Scarfo's keystrokes, the FBI was able to obtain his encryption keys and decrypt files that were later used in his prosecution for loan sharking and racketeering.[174]

C. What Are the Implications of Magic Lantern?

Many of the regulations that govern this new technology are contained in the U.S.A. Patriot Act.[175] Under current law, law enforcement agencies that want to infect a computer with this Trojan Horse virus must

164. Bob Port, *Spy Software Helps FBI Crack Encrypted Mail*, DAILY NEWS, Dec. 9, 2001, at 8. Sullivan, *supra* note 157. *See also FBI Confirms 'Magic Lantern' Exists*, MSNBC.com, Dec. 12, 2001, *available at* http://www.msnbc.com/news/671981.sap.

165. Lou Dolinar, *Upping the Pressure*; *With New Tools and Laws, Authorities Can Target Suspects' Computers with Accuracy*, NEWSDAY, Dec. 11, 2001 at C08.

166. See *id.*

167. Christopher Woo and Miranda So, *The Case for Magic Lantern: September 11 Highlights the Need for Increased Surveillance*, 15 HARV. J. LAW & TECH. 521, 524 (2002).

168. Dolinar, *supra* note 165.

169. Woo & So, *supra* note 167, at 524.

170. *Id.*

171. *See* Dolinar, *supra* note 165.

172. Sullivan, *supra* note 157.

173. *Id.*

174. Sullivan, *supra* note 157.

175. Vamosi, *supra* note 155.

acquire a court order allowing them to place the program on a suspect's computer.[176] Under the U.S.A. Patriot Act, however, only a state or U.S. attorney general need approve the measure to begin the process, while a court order can come later.

So far, Magic Lantern seems capable of curing many ills plaguing law enforcement. First and foremost, Magic Lantern turns the task of monitoring encrypted e-mail and other Internet traffic from a task that is nearly impossible to one as easy as obtaining approval. Second, the Fourth Amendment concerns raised by the FBI's Carnivore system are diminished because Magic Lantern is directed at specific computers or specific e-mails, thus eliminating the need to cast the net too wide. These factors, when coupled with a form of judicial oversight, will provide law enforcement with the tools they need to investigate suspects while adhering to constitutional guarantees.

D. Magic Lantern: Shining a Light on a New Solution

The advent of the Internet has revolutionized the world. Through this new medium we can check movie listings, look up new recipes, download the latest music, and read newspapers written halfway around the world. The Internet's most profound effect, however, lies in the booming market of e-commerce. Although the Internet contributed to record economic growth in the 1990s, that success was based on businesses ensuring the confidentiality of customers' personal information. American businesses accomplished this task domestically and overseas by using limited-strength encryption programs and later, when the government abolished regulations limiting the strength of encryption technology, stronger programs.

Although the abolition of encryption regulations proved necessary to e-commerce and helped vault the economy to record levels, the move had dire consequences on our national security. Businesses weren't the only organizations using encryption to keep communications from prying eyes. Terrorist organizations, such as al Qaeda, saw encryption as a vehicle to keep its plans secret and to carry out its acts of terrorism undetected.

It appears now that we have come full circle. The government began regulating encryption as munitions to ensure the technology would not fall into the hands of our enemies. Slowly, it backed down and relaxed the regulations to satisfy the needs of our evolving economy. As regulations relaxed, our economy strengthened, and so did terrorists' capabilities. Now that terrorists have access to the technology, what can be done to regulate it? The solution lies not in reviving old regulations, but in implementing

176. *See id.*

new technologies. As technology evolves, so too must the government's response to the problems new technology creates.

The government has responded by creating Magic Lantern, a new technology that protects business while ensuring the nation's security. Not only does Magic Lantern allow lax encryption regulation, but it also targets only those individuals who the government has probable cause to suspect of engaging in terrorist activities. It ensures privacy and protection for businesses while giving terrorists a false sense of security. Further, Magic Lantern should be governed by existing constitutional protections; thus, there would not be a need for additional regulations. Magic Lantern solves the problem of encryption regulation as it takes away the need to regulate encryption altogether.

VI. CONCLUSION

In the aftermath of September 11, 2001, many are struggling with the thought that terrorism can strike at home as easily as it can abroad. Terrorism is no longer carried out with grenades, Molotov cocktails, or pipe bombs. The terrorists of today employ computers, the Internet, cell phones, steganography, and encryption. Using this technology, terrorist groups can carry out their plans in secret, while intelligence agencies are left to conduct their investigations after the fact. Although the widespread dissemination of encryption in the absence of government regulation may affect national security, we still must examine the effects of governmental regulation on businesses and individuals before reacting. E-commerce powered by the Internet has helped drive the American economy to record levels. Its success could not have been accomplished, however, if customers' personal and private information could not be protected online by businesses. Past attempts at encryption regulation illustrate this is a delicate balance—a balance which has recently shifted in favor of business. While the business sector has won the battle, however, law enforcement is still effectively fighting the war with the development of new technologies that break the encryption barrier without raising the concerns of past regulatory efforts.