

WWW.STOPCYBERCRIME.COM: HOW THE USA PATRIOT ACT COMBATS CYBER-CRIME

Tammy J. Schemmel[†]

I.	INTRODUCTION	921
II.	COMPUTER-USE LEGISLATION	924
	A. <i>The USA PATRIOT Act</i>	925
	B. <i>The Computer Fraud and Abuse Act</i>	927
	C. <i>The Electronic Communications Privacy Act</i>	935
III.	CONCLUSION.....	948

I. INTRODUCTION

As government agencies and businesses rely more heavily on computer technology, the opportunities increase for cyber-criminals to do harm. The ever increasing cyber-crime problem begins with the fact that a person “with a standard desktop PC can potentially pose a real threat to [computer] systems”¹

According to the U.S. Census Bureau, in 2000, 51% of American households had computers and 41.5% of American households had Internet access.² Globally, about 304 million people have access to the Internet.³ These Internet consumers shop, search for jobs, and gather information online.⁴ In fact, in

[†] Minnesota State University Moorhead, B.S. International Business, B.A. Spanish, *magna cum laude*, 2001; William Mitchell College of Law, J.D. anticipated 2004.

1. Electronic Frontier Foundation, *RSA Code-Breaking Contest Again Won by Distributed.Net and Electronic Frontier Foundation (EFF)*, Jan. 19, 1999, at http://www.eff.org/Privacy/Crypto_misc/DESCracker/HTML/19990119_deschalenge3.html (last visited Aug. 25, 2002).

2. ERIC C. NEWBURGER, U.S. CENSUS BUREAU, HOME COMPUTERS AND INTERNET USE IN THE UNITED STATES: AUGUST 2000 1 (2001), *available at* <http://www.census.gov/prod/2001pubs/p23-207.pdf> (last visited Aug. 26, 2002). Fifty-four million households have a computer while forty-four million households have Internet access. *Id.* at 1-2.

3. U.S. DEP’T OF COMMERCE, DIGITAL ECONOMY 2000 7 (June 2000), *available at* <http://www.esa.doc.gov/de2000.pdf> (Sept. 2001).

4. *Id.* at 8.

the fourth quarter of 1999, the Census Bureau found that online retail sales totaled \$5.3 billion.⁵

More striking, an *Industry Standard* estimate forecasts the value of electronic transactions between businesses to range from \$634 billion to \$2.8 trillion in 2003.⁶ A *Purchase Magazine* survey found that 38% of companies use the Internet to conduct some of their business transactions.⁷ The survey also found that 35% of companies that did not do business over the Internet planned to start by 2000, and 54% of the companies that did not do business over the Internet planned to start by 2002.⁸

With so many people using the Internet and with the consistent growth of Internet business transactions, it is not surprising that the government would take strong measures to protect the Internet and other electronic forms of communication from intruders who damage computer systems.⁹ These intruders are called “crackers”¹⁰ (not to be confused with “hackers”¹¹) and

5. *Id.* at 9. The survey included only business-to-consumer goods retailers and left out business-to-consumer sales of services (travel, entertainment, or stock transactions). *Id.* at 9 n.5.

6. *Id.* at 15. See Stacy Lawrence, *Behind the Numbers: The Mystery of B2B Forecasts Revealed*, THE INDUSTRY STANDARD, Feb. 21, 2000, available at <http://www.thestandard.com/article/0,1902,11300,00.html> (June 2000).

7. U.S. DEP'T OF COMMERCE, *supra* note 3, at 16.

8. *Id.*

9. Thomas R. McCarthy, *Don't Fear Carnivore: It Won't Devour Individual Privacy*, 66 MO. L. REV 827, 831 (2001).

If law enforcement is too timid in responding to cybercrime . . . we will, in effect, render cyberspace a safe haven for criminals and terrorists to communicate and carry out crime, without fear of authorized government surveillance. If we fail to make the Internet safe, people's confidence in using the Internet and e-commerce will decline, endangering the very benefits brought by the Information Age. Proper balance is key.

Id.

10. See SearchSecurity.com Definitions, at http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci211852,00.html (last visited Aug. 29, 2002). It defines “cracker” as:

[S]omeone who breaks into someone else's computer system, often on a network; bypasses passwords or licenses in computer programs; or in other ways intentionally breaches computer security. A cracker can be doing this for profit, maliciously, for some altruistic purpose or cause, or because the challenge is there. Some breaking-and-entering has been done ostensibly to point out weaknesses in a site's security system. The term ‘cracker’ is not to be confused with ‘hacker.’ Hackers generally deplore cracking.

Id.

11. See SearchSecurity.com Definitions, at

they are becoming more of a problem with the increasing use of computers. For example, after the North Atlantic Treaty Organization (“NATO”) jets hit the Chinese Embassy in Belgrade in May of 1999, crackers from China attacked a handful of U.S. government sites.¹² In an unrelated incident, the U.S. Justice Department’s website was shut down because crackers put Nazi swastikas on its homepage.¹³ Crackers have also damaged the CIA’s website by changing the name from “Central Intelligence Agency” to “Central Stupidity Agency.”¹⁴

These acts seem harmless enough and most “break-ins are done purely as sport”¹⁵ A problem arises, however, when crackers break into systems for “greed, or for foreign powers, or for one industry against another, or for organized crime.”¹⁶ It is estimated that Internet crime takes about \$1.6 trillion out of the global economy.¹⁷ This is due to such things as website downtime, website repair, the cost of training computer crime trackers, and lost business.¹⁸

In the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (“USA PATRIOT Act”), Congress attempted to give

http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci212220,00.html (last visited Oct. 26, 2002). It defines “hacker” as “a clever programmer.”

[F]ive possible characteristics qualify one as a hacker: (1) [a] person who enjoys learning details of a programming language or system; (2) [a] person who enjoys actually doing the programming rather than just theorizing about it; (3) [a] person capable of appreciating someone else’s hacking; (4) [a] person who picks up programming quickly; and (5) [a] person who is an expert at a particular programming language or system.

Id.

12. The Associated Press and Reuters, *Feds Warn Hackers will be Prosecuted; Pro-Mitnick Protest Planned*, available at <http://www.cnn.com/TECH/computing/9906/02/hunting.hackers> (June 2, 1999).

13. *Id.*

14. *Id.*

15. San Francisco Examiner, *FBI Uses Computers to Catch High-Tech Crooks*, The News and Observer Publishing Co. 1995, available at <http://www.indy.net/~sabronet/news/fbihack.html> (last visited Aug. 29, 2002).

16. *Id.*

17. Reuters, *FBI Plan: Cybercrime Info Sharing*, at <http://cert.uni-stuttgart.de/archive/isn/2001/01/msg00024.html> (Jan. 5, 2001).

18. See Heather Eikenberry, *Hacker’s Insurance: When All Else Fails*, SANS INST. INFO. READING ROOM, at <http://ir.sans.org/casestudies/insurance.php> (Jan. 9, 2001). In 2000, Computer Security Institute (CSI) reported an increase in computer crime. *Id.*

government agencies the leeway they need to track down cyber-criminals.¹⁹ This Comment explores the history of computer-use legislation and documents the relevant sections of the USA PATRIOT Act that amend sections of the Computer Fraud and Abuse Act and sections of the Electronic Communications Privacy Act.²⁰ Next, the Comment analyzes the effects of such legislation on computer users and law enforcement agencies.²¹ The Comment concludes that the legislation is a necessary evil in the quest to track down and punish cyber-criminals.²²

II. COMPUTER-USE LEGISLATION

In the past two decades, Congress has passed a number of acts that regulate computer use and privacy.²³ This Comment addresses only a few of the statutes that have been amended by the USA PATRIOT Act.²⁴ A discussion of certain sections of the Computer

19. The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001) [hereinafter "USA PATRIOT Act"].

20. See *infra* Part II.

21. *Id.*

22. See *infra* Part III. This Comment does not address civil liberties issues. For articles critical of the USA PATRIOT Act on civil liberty grounds see Jennifer C. Evans, Comment, *Hijacking Civil Liberties: The USA PATRIOT Act of 2001*, 33 LOY. U. CHI. L.J. 933, 974-82 (2002); Steven A. Osher, *Privacy, Computers and the PATRIOT Act: The Fourth Amendment Isn't Dead, But No One Will Insure It*, 54 FLA. L. REV. 521, 525-26 (2002); Walter Shapiro, *Usual Adversaries United Over Threat to Liberties*, USA TODAY, Sept. 26, 2001, at A6; Electronic Frontier Foundation, *EFF Analysis of the Provisions of the USA PATRIOT Act That Relate to Online Activities*, at http://www.eff.org/Privacy/Surveillance/Terrorism_militias/20011031_eff_usa_patriot_analysis.html (Oct. 31, 2001); Karen G. Schneider, *The Patriot Act: Last Refuge of a Scoundrel*, AMERICAN LIBRARIES, at <http://www.ala.org/online/netlib/il302.html> (Mar. 2002); but see Michael T. McCarthy, *USA PATRIOT Act*, 39 HARV. J. ON LEGIS. 435, 451-52 (2002) ("In the debate over the USA PATRIOT Act, one should not lose sight of the fact that the law itself does not take away civil liberties, although some of its provisions permit the executive branch to take actions that may do so.").

23. For a comprehensive look at the statutory language of the Electronic Communications Privacy Act, the Communications Act, the Foreign Intelligence Surveillance Act, and the Computer Fraud & Abuse Act before and after the enactment of the USA PATRIOT Act see Kay Pauley, *Showing How Key Provisions of the USA PATRIOT Act (P.L. 107-56) Amend Existing Law*, at http://www.cdt.org/security/USA_PATRIOT_Actpatriot/title1.pdf (Nov. 2001).

24. Statutes such as the Copyright Infringement Act, the No Electronic Theft Act, the Digital Millennium Copyright Act, the National Stolen Property Act, the Communications Decency Act of 1996, the Child Online Protection Act of 1998, and the Internet False Identification Act of 2000 will not be discussed. For a discussion of such statutes and how they relate to computer crime, see Heather

Fraud and Abuse Act and the Electronic Communications Privacy Act in their pre-USA PATRIOT Act form follows. Subsequent to those discussions is an assessment of how the USA PATRIOT Act has changed each statute and an evaluation of the effects those changes have on computer users and law enforcement agencies.

A. *The USA PATRIOT Act*

President George W. Bush signed the USA PATRIOT Act of 2001 into law on October 26, 2001, just six weeks after the attacks of September 11, 2001.²⁵ The PATRIOT Act originated in the House of Representatives²⁶ and the USA Act originated in the Senate.²⁷ On October 24, 2001, the House passed House Bill 3162, which integrated House Bill 2975 and Senate Bill 1510.²⁸ The Senate also passed the bill and sent it to President Bush to sign.²⁹ The bill was hurried through Congress in hopes of preventing future attacks.³⁰

Jacobson & Rebecca Green, *Computer Crimes*, 39 AM. CRIM. L. REV. 273 (2002).

25. USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (2001). The Act consists of ten provisions:

Title I—Enhancing Domestic Security Against Terrorism;

Title II—Enhanced Surveillance Procedures;

Title III—International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001;

Title IV—Protecting the Border;

Title V—Removing Obstacles to Investigating Terrorism;

Title VI—Providing for Victims of Terrorism, Public Safety Officers, and Their Families;

Title VII—Increased Information Sharing for Critical Infrastructure Protection;

Title VIII—Strengthening the Criminal Laws Against Terrorism;

Title IX—Improved Intelligence; and

Title X—Miscellaneous.

Id.

26. CHARLES DOYLE, CRS REPORT FOR CONGRESS, THE USA PATRIOT ACT: A LEGAL ANALYSIS I (2002), available at

<http://fpc.state.gov/documents/organization/10092.pdf> (last visited Dec. 22, 2002) [hereinafter “CRS REPORT FOR CONGRESS”]. Representative Sensenbrenner for himself and Representatives Conyers, Hyde, Coble, Goodlatte, Jenkins, Jackson-Lee, Cannon, Meehan, Graham, Bachus, Wexler, Hostettler, Keller, Issa, Hart, Flake, Schiff, Thomas, Goss, Rangel, Berman, and Lofgren introduced the PATRIOT Act in the House of Representatives as House Bill 2975. *Id.* at 1 n.2.

27. *Id.* Senator Daschle for himself and Senators Lott, Leahy, Hatch, Graham, Shelby, and Sarbanes introduced the USA Act in the Senate as Senate Bill 1510. *Id.* at 1 n.2.

28. *Id.* at 1.

29. *Id.* at 1-2.

30. See *Homeland Defense: Hearing Before the Senate Comm. on the Judiciary*, 107th Cong. (Sept. 25, 2001) (statement of Attorney General John Ashcroft) (“Everyday

The primary stated purposes of the USA PATRIOT Act are to “deter and punish terrorist acts in the United States and around the world [and] to enhance law enforcement investigatory tools”³¹ The USA PATRIOT Act fulfills its purposes mainly by amending pre-existing statutes.³² Amendments to some statutes produce an effect greater than catching terrorists.³³ The amended Computer Fraud and Abuse Act and the amended Electronic Communications Privacy Act, for example, give law enforcement officials more latitude in catching domestic cyber-criminals.³⁴

In his testimony before the House Committee on the Judiciary, Attorney General John Ashcroft commented on how the USA PATRIOT Act would be designed to meet its purposes. He noted that one deficiency in our current laws was that “technology has dramatically outpaced our statutes.”³⁵ He then stated, as the first objective of the USA PATRIOT Act, “law enforcement needs a

that passes with outdated statutes and old rules of engagement is a day that terrorists have a competitive advantage.”) *available at* <http://judiciary.senate.gov/oldsite/te092501f.htm> (last visited Oct. 26, 2002).

31. USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (2001).

32. *See id.*

33. In a hearing before the House Committee on the Judiciary, while discussing whether the legislation should be limited to terrorists and not crimes in general, Michael Chertoff, Assistant Attorney General in the Justice Department for the Criminal Division, noted that:

[W]hen you commence a criminal investigation, it doesn't come labeled terrorist or nonterrorist. In fact, this provision, and a number of the provisions really address inconsistencies in the law where under one type of technology we are able to do one thing, but emerging technology has created a gap in the law. There's no change in the privacy protection substantively. We're just trying to even the playing field.

Administration's Draft Anti-Terrorism Act of 2001: Hearing Before the Comm. on the Judiciary, 107th Cong. 26 (2001) (DoJ at § 108), available at <http://www.house.gov/judiciary/75288.pdf> (last visited, Dec. 22, 2002) [hereinafter “DoJ”].

In the same hearing, while discussing whether computer crimes could rise to the level of terrorism, Attorney General John Ashcroft stated:

[W]hen you think about the utilization of computers in terms of air traffic control, you can imagine the chaos that could come from the disruption of that system if we had an assault launched through a computer virus or some other infection in the computer infrastructure, whether it be power grids, power generation supplies and the like.

Id. at 18.

34. *See infra* Parts II.B-C.

35. United States Department of Justice, *Attorney General John Ashcroft Testimony Before the House Committee on the Judiciary*, at http://www.usdoj.gov/ag/agcrisisremarks9_24.htm (Sept. 24, 2001).

strengthened and streamlined ability for our intelligence-gathering agencies to gather the information necessary to disrupt, weaken and eliminate the infrastructure of terrorist organizations.”³⁶ Attorney General Ashcroft’s support for this objective is noted throughout this Comment.

The USA PATRIOT Act amended the Computer Fraud and Abuse Act and the Electronic Communications Privacy Act to work more effectively with current technology. Both Acts provide examples of how Attorney General Ashcroft’s objective will be met.

B. *The Computer Fraud and Abuse Act*

The Computer Fraud and Abuse Act³⁷ (“CFAA”) was the first law to address computer crime and is the main federal cyber-crime statute.³⁸ The CFAA addresses “computer crimes in which the computer is the ‘subject’—that is, computer crimes for which there is no analogous traditional crime and for which special legislation is needed.”³⁹ Such crimes include the use of “sniffers,”⁴⁰ “worms,”⁴¹

36. *Id.*

37. 18 U.S.C. § 1030 (1984). The 1984 Act was narrow, but as new computer crime issues arose, Congress expanded the scope of the law by enacting the Computer Fraud and Abuse Act of 1986. *See* Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, § 2, 100 Stat. 1213 (1986) (current version at 18 U.S.C. § 1030 (2002)). *See also* Dodd S. Griffith, Note, *The Computer Fraud and Abuse Act of 1986: A Measured Response to a Growing Problem*, 43 VAND. L. REV. 453, 474 (1990) (discussing the history of the 1984 Act and its 1986 amendments). Congress expanded the Act’s scope again in 1988, 1989, 1990, 1994, and 1996. *See* Anti-Drug Abuse Act of 1988, Pub. L. No. 100-690, Title VII, § 7065, 102 Stat. 4404 (1988) (current version at 18 U.S.C. § 1030 (2002)); Financial Institutions Reform Recovery and Enforcement Act of 1989, Pub. L. No. 101-73, Title IX, § 962(a)(5), 103 Stat. 502 (1989) (current version at 18 U.S.C. § 1030 (2002)); Crime Control Act of 1996, Pub. L. No. 101-647, Title XII, § 1205(e), Title XXV, § 2597(j), Title XXXV, § 3533, 104 Stat. 4831, 4910, 4925 (1990) (current version at 18 U.S.C. § 1030 (2002)); Violent Crime Control and Law Enforcement Act of 1994, Pub. L. No. 103-322, Title XXIX, § 290001(b)-(f), 108 Stat. 2097-99 (1994) (current version at 18 U.S.C. § 1030 (2002)); Economic Espionage Act of 1996, Pub. L. No. 104-294, Title II, § 201, Title VI, § 604(b)(36), 110 Stat. 3491, 3508 (1996) (current version at 18 U.S.C. § 1030 (2002), as amended by USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (2001)). *See also* Jo-Ann M. Adams, Comment, *Controlling Cyberspace: Applying the Computer Fraud and Abuse Act to the Internet*, 12 SANTA CLARA COMPUTER & HIGH TECH. L.J. 403, 424-25 (1996) (highlighting changes made by the 1988, 1989, and 1990 amendments).

38. Bill Reilly, *The Impact of the USA PATRIOT Act on Network Security Practices*, at <http://packetstormsecurity.nl/papers/legal/patriot.doc> (Nov. 15, 2001).

39. Jacobson & Green, *supra* note 24, at 279; *see* NATIONAL INSTITUTE OF JUSTICE, U.S. DEP’T OF JUSTICE, COMPUTER CRIME: CRIMINAL JUSTICE RESOURCE MANUAL 2 (1989).

“Trojan horses,”⁴² “logic bombs,”⁴³ and “viruses.”⁴⁴ The CFAA has been used to prosecute “malicious code authors, . . . ‘outside’ hackers who penetrate computers, steal information and/or cause damage to the system, and people who use computers to commit fraud.”⁴⁵

1. 18 U.S.C. § 1030 Pre-USA PATRIOT Act

The CFAA prohibits a person from knowingly accessing a computer or exceeding authorization to gain information concerning national defense, foreign relations, or any other restricted data that could be used to injure the United States, or that could be used to the advantage of any foreign nation.⁴⁶ The CFAA also makes it illegal for a person, without authorization, to intentionally obtain information contained in the records of a financial institution or consumer-reporting agency.⁴⁷ An unauthorized person cannot intentionally obtain information from any department or agency of the United States⁴⁸ or from any protected computer if the conduct involves an interstate or foreign communication.⁴⁹ The CFAA also makes it illegal to access a nonpublic computer of any department or agency of the United

40. See SANS INSTITUTE RESOURCES, NSA GLOSSARY OF TERMS USED IN SECURITY AND INTRUSION DETECTION, at <http://www.sans.org/newlook/resources/glossary.htm> (last visited Sept. 27, 2002) (defining “sniffer” as “[a] program to capture data across a computer network. Used by hackers to capture user id names and passwords; [s]oftware tool that audits and identifies network traffic packets. [It] is also used legitimately by network operations and maintenance personnel to troubleshoot network problems”).

41. See *id.* (defining “worm” as an “[i]ndependent program that replicates from machine to machine across network connections often clogging networks and information systems as it spreads”).

42. See *id.* (defining “Trojan horse” as “[a]n apparently useful and innocent program containing additional hidden code which allows the unauthorized collection, exploitation, falsification, or destruction of data”).

43. See *id.* (defining “logic bomb,” also known as “fork bomb,” as “[a] resident computer program which, when executed, checks for a particular condition or particular state of the system which, when satisfied, triggers the perpetration of an unauthorized act”).

44. See *id.* (defining “virus” as “[a] program that can ‘infect’ other programs by modifying them to include a, possibly evolved, copy of itself”).

45. See Reilly, *supra* note 38.

46. 18 U.S.C. § 1030(a)(1).

47. *Id.* at (a)(2)(A).

48. *Id.* at (a)(2)(B).

49. *Id.* at (a)(2)(C).

States or any computer used by the United States government if that conduct affects the government's use.⁵⁰ Beyond minor exceptions, a person cannot access a protected computer to further an intended fraud.⁵¹

The Act prohibits a person, with the intent to defraud, from trafficking⁵² passwords that would affect interstate and foreign commerce⁵³ or permit access to a computer used by or for the United States Government.⁵⁴ Finally, a person cannot transmit through interstate or foreign commerce a threat to damage a protected computer in order to extort something of value.⁵⁵

2. 18 U.S.C § 1030 Post-USA PATRIOT Act

Section 814 of the USA PATRIOT Act amended and clarified the CFAA in a number of significant ways. One notable change was to subsection (a)(5),⁵⁶ the computer "cracker"⁵⁷ subsection. Before the USA PATRIOT Act, subsection (a)(5) had three sub-subsections: sub-subsection (A) prohibited a person from intentionally accessing and intentionally causing damage to a protected computer through the transmission of a program, information, code, or command;⁵⁸ sub-subsection (B) prohibited a person from intentionally accessing and recklessly causing damage through access of a protected computer;⁵⁹ and sub-subsection (C) prohibited a person from intentionally accessing and causing damage to a protected computer.⁶⁰

The USA PATRIOT Act changed several original sub-subsections⁶¹ and added new sub-subsections, (a)(5)(B)(i-v),⁶² that

50. *Id.* at (a)(3).

51. *Id.* at (a)(4).

52. To "traffic" is to "transfer or otherwise dispose of, to another, or obtain control of with intent to transfer or dispose of." 18 U.S.C. § 1029(e)(5).

53. 18 U.S.C. § 1030(a)(6)(A).

54. *Id.* at (a)(6)(B).

55. *Id.* at (a)(7). The USA PATRIOT Act section 814(d)(5), 115 Stat. 272, 384 now defines "person" as "any individual, firm, corporation, educational institution, financial institution, governmental entity, or legal or other entity."

56. 18 U.S.C § 1030(a)(5), *amended by* USA PATRIOT Act § 814(a), 115 Stat. 272, 382-83.

57. *See* SearchSecurity.com Definitions, *supra* note 10.

58. 18 U.S.C. § 1030(a)(5)(A).

59. *Id.* at (a)(5)(B).

60. *Id.* at (a)(5)(C).

61. The USA PATRIOT Act changed original sub-subsections (a)(5)(A), (a)(5)(B), and (a)(5)(C) to (a)(5)(A)(i), (a)(5)(A)(ii), and (a)(5)(A)(iii), respectively.

closely resemble what previously were sub-subsections (e)(8)(A-D).⁶³ The new provisions prohibit the conduct of (a)(5)(A) where the damage either: (i) caused the loss of at least \$5000 to one or more persons during any one-year period;⁶⁴ (ii) modified or impaired a medical examination, diagnosis, treatment, or care of one or more individuals;⁶⁵ (iii) caused physical injury to any person;⁶⁶ (iv) caused a threat to public health or safety;⁶⁷ or (v) caused damage to a computer system used by or for the government in furtherance of the administration of justice, national defense, or national security.⁶⁸

Sub-subsections (e)(8)(A)-(D) were part of the statute's definition of damages. By removing sub-subsections (A)-(D) and moving them to sub-subsections (a)(5)(B)(i)-(v), the USA PATRIOT Act has broadened the definition of "damages."⁶⁹ The effect of the change "is to prohibit and punish crimes under this section that cause minimal damage and to increase the punishment for crimes causing significant damage."⁷⁰

Before enactment of the USA PATRIOT Act, a person charged with violating sub-subsection (a)(5) or sub-subsection (a)(7) could have argued that damages did not exceed \$5000 in one year.⁷¹ A person charged with violating amended sub-subsection (a)(7) can no longer make such an argument because there are no specifications on the amount of damages that must be sustained.⁷² However, the USA PATRIOT Act did not clarify how damages would be calculated. A proper calculation is necessary because

62. 18 U.S.C. § 1030(a)(5)(B), *amended by* USA PATRIOT Act § 814(a)(4), 115 Stat. 272, 383.

63. *Id.* at (e)(8)(A-D), *amended by* USA PATRIOT Act § 814(d)(3), 115 Stat. 272, 384.

64. *Id.* at (a)(5)(B)(i), *amended by* USA PATRIOT Act § 814(a)(4), 115 Stat. 272, 383.

65. *Id.* at (a)(5)(B)(ii), *amended by* USA PATRIOT Act § 814(a)(4), 115 Stat. 272, 383.

66. *Id.* at (a)(5)(B)(iii), *amended by* USA PATRIOT Act § 814(a)(4), 115 Stat. 272, 383.

67. *Id.* at (a)(5)(B)(iv), *amended by* USA PATRIOT Act § 814(a)(4), 115 Stat. 272, 383.

68. *Id.* at (a)(5)(B)(v), *amended by* USA PATRIOT Act § 814(a)(4), 115 Stat. 272, 383.

69. *Id.* at (e)(8), *amended by* USA PATRIOT Act § 814(d)(3), 115 Stat. 272, 384 (defining "damages" as "any impairment to the integrity or availability of data, a program, a system, or information").

70. Jacobson & Green, *supra* note 24, at 283.

71. *See id.* at 285.

72. *See supra* note 69 (defining "damages").

according to sub-subsection (a)(5)(B)(i), the damage sustained must value \$5000 to one or more persons within a one-year period.⁷³

The next notable addition to the CFAA is to the definition of “protected computer.”⁷⁴ A “protected computer” is a computer that is used exclusively by a financial institution or by the United States government⁷⁵ or one that is used in interstate or foreign commerce or communications.⁷⁶ The USA PATRIOT Act added to the definition of “protected computers” any “computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States.”⁷⁷

By extending the definition of “damages” and “protected computer,” Congress has effectively given the United States Secret Service and other governmental agencies greater jurisdiction to investigate computer crimes.⁷⁸ Sub-subsections (a)(4), (a)(5), and (a)(7) contain the words “protected computers” giving the Secret Service the power to investigate any computer fraud case in which the perpetrator intentionally, and with the intent to defraud, accesses a protected computer, furthers an intended fraud, and obtains anything of value.⁷⁹ This is only true if the fraud affects interstate or foreign commerce or communication of the United States.⁸⁰ The Secret Service would also have the power to investigate any computer cracking scheme that affects interstate and foreign commerce or communications of the United States as long as the minimum requirements of sub-subsection (a)(5)(B) are met.⁸¹

The USA PATRIOT Act also strengthened the punishment⁸²

73. 18 U.S.C. § 1030(a)(5)(B)(i), *amended by* USA PATRIOT Act § 814(a)(4), 115 Stat. 272, 383.

74. *Id.* at (e)(2), *amended by* USA PATRIOT Act § 814(d)(1), 115 Stat. 272, 384.

75. *Id.* at (e)(2)(A).

76. *Id.* at (e)(2)(B), *amended by* USA PATRIOT Act § 814(d)(1), 115 Stat. 272, 384.

77. *Id.*

78. *See id.* at (d). The United States Secret Service, and other agencies, have the authority to investigate any offenses under sub-subsections (a)(2)(A), (a)(2)(B), (a)(3), (a)(4), and (a)(6). *Id.*

79. *See* 18 U.S.C. § 1030(a)(4).

80. *See id.*

81. *See id.* at (a)(5).

82. This table illustrates the statutory punishment for violations of specific sub-subsections before and after the enactment of the USA PATRIOT Act. Its

purpose is to facilitate a clear understanding of the analysis in the subsequent paragraphs of the text.

Punishment for Violation of 18 U.S.C. § 1030

CFAA Section and Subsection Reference to Targeted Offense	CFAA Section and Subsection that Provides for Punishment	Pre-USA PATRIOT Act Punishment for Violation	Post-USA PATRIOT Act Punishment for Violation
18 U.S.C. § 1030(a)(1)	1 st Offense— 18 U.S.C. § 1030(c)(1)(A) 2 nd Offense— 18 U.S.C. § 1030(c)(1)(B)	1 st Offense—fine and/or imprisonment for not more than 10 years 2 nd Offense—fine and/or imprisonment for not more than 20 years	Same
18 U.S.C. § 1030(a)(2)	1 st Offense— 18 U.S.C. § 1030(c)(2)(A)-(B) 2 nd Offense— 18 U.S.C. § 1030(c)(2)(C)	1 st Offense—fine and/or imprisonment for not more than 1 year or 5 years depending on how or why the crime was committed 2 nd Offense—fine and/or imprisonment for not more than 10 years	Same
18 U.S.C. § 1030(a)(3)	1 st Offense— 18 U.S.C. § 1030(c)(2)(A) 2 nd Offense— 18 U.S.C. § 1030(c)(2)(C)	1 st Offense—fine and/or imprisonment for not more than 1 year 2 nd Offense—fine and/or imprisonment for not more than 10 years	Same
18 U.S.C. § 1030(a)(4)	1 st Offense— 18 U.S.C. § 1030(c)(3)(A) 2 nd Offense— 18 U.S.C. § 1030(c)(3)(B)	1 st Offense—fine and/or imprisonment for not more than 5 years 2 nd Offense—fine and/or imprisonment for not more than 10 years	Same
18 U.S.C. § 1030(a)(5)(A)(i)	1 st Offense— 18 U.S.C. § 1030(c)(4)(A) 2 nd Offense— 18 U.S.C. § 1030(c)(4)(C)		1 st Offense—fine and/or imprisonment for not more than 10 years 2 nd Offense—fine and/or imprisonment for not more than 20 years

for violation or attempted violation⁸³ of subsection (a). The Act “directs the U.S. Sentencing Commission to amend the U.S.S.G. to ensure that individuals convicted under 18 U.S.C. § 1030 ‘can be subjected to appropriate penalties, without regard to any mandatory minimum term of imprisonment.’”⁸⁴ It also strengthened the punishment in part by stating that the word “conviction” includes any conviction under state law.⁸⁵

A person who violates sub-subsection (a)(1) can be fined

18 U.S.C. § 1030(a)(5)(A)(ii)	1 st Offense— 18 U.S.C. § 1030(c)(4)(B) 2 nd Offense— 18 U.S.C. § 1030(c)(4)(C)		1 st Offense—fine and/or imprisonment for not more than 5 years 2 nd Offense—fine and/or imprisonment for not more than 20 years
18 U.S.C. § 1030(a)(5)(A)(iii)	1 st Offense— 18 U.S.C. § 1030(c)(2)(A) 2 nd Offense— 18 U.S.C. § 1030(c)(3)(B)		1 st Offense—fine and/or imprisonment for not more than 1 year 2 nd Offense—fine and/or imprisonment for not more than 10 years
18 U.S.C. § 1030(a)(6)	1 st Offense— 18 U.S.C. § 1030(c)(2)(A) 2 nd Offense— 18 U.S.C. § 1030(c)(2)(C)	1 st Offense—fine and/or imprisonment for not more than 1 year 2 nd Offense—fine and/or imprisonment for not more than 10 years	Same
18 U.S.C. § 1030(a)(7)	1 st Offense— 18 U.S.C. § 1030(c)(3)(A) 2 nd Offense— 18 U.S.C. § 1030(c)(3)(B)	1 st Offense—fine and/or imprisonment for not more than 5 years 2 nd Offense—fine and/or imprisonment for not more than 10 years	Same

83. 18 U.S.C. § 1030(b). “Whoever attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section.” *Id.*

84. Jacobson & Green, *supra* note 24, at 287 (quoting USA PATRIOT Act § 814(f), 115 Stat. 272, 384) (amending 28 U.S.C. § 994(p)).

85. 18 U.S.C. § 1030(e)(10), *amended by* USA PATRIOT Act § 814(d)(5), 115 Stat. 272, 384 (providing that the term “conviction” shall include “a conviction under the law of any State for a crime punishable by imprisonment for more than 1 year, an element of which is unauthorized access, or exceeding authorized access, to a computer.”).

and/or imprisoned for up to ten years.⁸⁶ On the second violation, that person can be fined and/or imprisoned for up to twenty years.⁸⁷ A person who violates sub-subsection (a)(2), (a)(3), (a)(5)(A)(iii), or (a)(6) can be fined and/or imprisoned for up to one year.⁸⁸ For violation of sub-subsection (a)(2),⁸⁹ punishment is maximized at a fine and/or five years in prison if: (1) the offense was committed for purposes of commercial advantage or private financial gain;⁹⁰ (2) the offense was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any state;⁹¹ or (3) the value of the information obtained exceeds \$5000.⁹² Maximum sentences under sub-subsections (a)(2), (a)(3), and (a)(6) are set at ten years for second-time offenders.⁹³

A person who violates sub-subsection (a)(4), (a)(5)(A)(iii), or (a)(7) can be fined and/or imprisoned for up to five years.⁹⁴ On the second offense, punishment is a fine and/or imprisonment for up to ten years.⁹⁵ The USA PATRIOT Act adds to the CFAA that a violation under sub-subsection (a)(5)(A)(i) will result in a fine and/or imprisonment up to ten years.⁹⁶ A violation of sub-subsection (a)(5)(A)(ii) results in a fine and/or imprisonment of up to five years.⁹⁷ For each of these offenses the punishment is maximized at a fine and/or imprisonment for up to twenty years for the second offense.⁹⁸

The next notable change to the CFAA is found in the added definition of "loss."⁹⁹ The broad definition is important because a

86. *Id.* at (c)(1)(A).

87. *Id.* at (c)(1)(B).

88. *Id.* at (c)(2)(A).

89. *Id.* at (c)(2)(B). The punishment is also for an attempt to commit an offense under subsection (c)(2)(A). *Id.*

90. *Id.* at (c)(2)(B)(i).

91. *Id.* at (c)(2)(B)(ii).

92. *Id.* at (c)(2)(B)(iii).

93. *Id.* at (c)(2)(C).

94. *Id.* at (c)(3)(A).

95. *Id.* at (c)(3)(B).

96. *Id.* at (c)(4)(A), amended by USA PATRIOT Act § 814(c)(3), 115 Stat. 272, 383.

97. *Id.* at (c)(4)(B), amended by USA PATRIOT Act § 814(c)(3), 115 Stat. 272, 383.

98. *Id.* at (c)(4)(C), amended by USA PATRIOT Act § 814(c)(3), 115 Stat. 272, 383.

99. *Id.* at (e)(11), amended by USA PATRIOT Act § 814(d)(5), 115 Stat. 272, 384 (defining "loss" as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the

person who suffers “damage or loss” by any violation of sub-subsections (a)(5)(B)(i)-(v) can bring a civil action against the violator to obtain compensatory damages, injunctive relief, or other equitable relief.¹⁰⁰ Damages for violation of sub-subsection (a)(5)(B)(i) are limited to economic damages.¹⁰¹ This should encourage people who would normally not bring a claim against the perpetrator to bring a claim. Likewise, it could lead to more prosecutions for cyber-crime, thereby creating a deterrent for future cyber-crime.

C. *The Electronic Communications Privacy Act*

The Electronic Communications Privacy Act¹⁰² (“ECPA”) is the federal law that protects electronic communication users against unauthorized interception, use, or disclosure of electronic communications while in transit or in storage.¹⁰³ The ECPA’s purpose is to update privacy protections and standards with the changes in computer and telecommunications technologies.¹⁰⁴ Since its inception, additional technology updates have included electronic mail (e-mail), the Internet, cellular phones (some with wireless Internet connections), and paging devices.¹⁰⁵

1. *18 U.S.C § 2702*

Section 2702 provides for voluntary disclosure by electronic communication service providers of customer communications or records.¹⁰⁶ This section prohibits a service provider from divulging the contents of a communication to any person.¹⁰⁷ The same

data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service”).

100. *Id.* at (g).

101. *Id.*

102. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848.

103. Seth Richard Lesser, *Privacy Law in the Internet Era: New Developments and Directions*, 701 PRACTICING L. INST. 115, 152-53 (June 2002).

104. See S. REP. No. 99-541, at 20-23 (1986); Henry M. Cooper, *The Electronic Communications Privacy Act: Does the Answer to the Internet Information Privacy Problem Lie in a Fifteen-Year-Old Federal Statute? A Detailed Analysis*, 20 J. MARSHALL J. COMPUTER & INFO. L. 1, 2 (Fall 2001).

105. Cooper, *supra* note 104, at 2.

106. 18 U.S.C. § 2702 (2000).

107. *Id.* at (a)(1). An “electronic communication service” is defined as “any service which provides to users thereof the ability to send or receive wire or

applies to remote computing service providers.¹⁰⁸ The USA PATRIOT Act adds sub-subsection (a)(3) to section 2702. It states generally that a provider of electronic communications service cannot divulge information about a customer.¹⁰⁹

The section has a few exceptions for disclosure of communications. For example, a provider may divulge the contents of a communication to the intended recipient,¹¹⁰ to a person who forwards it to its destination,¹¹¹ or to a law enforcement agency¹¹² if the contents were inadvertently obtained¹¹³ and appear to pertain to the commission of a crime.¹¹⁴

The USA PATRIOT Act added that a provider could divulge customer records to a law enforcement agency if the provider reasonably believes that immediate danger of death or serious bodily injury to any person requires disclosure.¹¹⁵ The USA PATRIOT Act also added that a provider can disclose customer information: (1) with consent of the customer;¹¹⁶ (2) as necessary to protect the provider;¹¹⁷ (3) to a governmental agency in the case of an emergency involving death or serious bodily injury;¹¹⁸ or (4) to any person other than a governmental agency.¹¹⁹

This new section allows “communications providers to disclose non-content information (such as the subscriber’s login records).”¹²⁰ Before the Act, a communications provider was

electronic communications[.]” 18 U.S.C. § 2510(15). An “electronic communication” is defined as “any transfer of sign, signals, writing, images, sound, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce. . . .” *Id.* at (12).

108. 18 U.S.C. § 2702(a)(2).

109. *Id.* at (a)(3), amended by USA PATRIOT Act § 212(a)(1)(B), 115 Stat. 272, 284.

110. *Id.* at (b)(1).

111. *Id.* at (b)(4).

112. *Id.* at (b)(6).

113. *Id.* at (b)(6)(A)(i).

114. *Id.* at (b)(6)(A)(ii).

115. *Id.* at (b)(6)(C), amended by USA PATRIOT Act § 212(a)(1)(D), 115 Stat. 272, 284.

116. *Id.* at (c)(2), amended by USA PATRIOT Act § 212(a)(1)(E), 115 Stat. 272, 284.

117. *Id.* at (c)(3), amended by USA PATRIOT Act § 212(a)(1)(E), 115 Stat. 272, 284.

118. *Id.* at (c)(4), amended by USA PATRIOT Act § 212(a)(1)(E), 115 Stat. 272, 285.

119. *Id.* at (c)(5), amended by USA PATRIOT Act § 212(a)(1)(E), 115 Stat. 272, 285.

120. CHARLES DOYLE, TERRORISM: SECTION BY SECTION ANALYSIS OF THE USA

expressly permitted to release content information, but not non-content information.¹²¹ Therefore, it permits the disclosure of less protected information.¹²²

2. 18 U.S.C. § 2703

This section focuses on the required disclosure of customer communications or records.¹²³ It requires electronic communication providers to disclose to a governmental agency the contents of electronic or wire communication that is in electronic storage for 180 days or less.¹²⁴ The investigators must have a warrant issued under the Federal Rules of Criminal Procedure.¹²⁵ Federal Rule of Criminal Procedure 41 requires that the “property” to be obtained “be within the district” of the issuing court.¹²⁶ Moreover, the statute did not allow warrants for e-mail located in other districts.¹²⁷

One way in which Attorney General Ashcroft supported his objective of giving law enforcement leeway in eliminating terrorist organizations was to provide a single order that would apply to all electronic communication providers:

[o]ur proposal would allow a federal court to issue a single order that would apply to all providers in the communications chain, including those outside the region where the court is located. We need speed in identifying and tracking down terrorists. Time is of the essence. The ability of law enforcement to trace communications into jurisdictions without obtaining an additional court order can be the difference between life and death for American citizens.¹²⁸

To further this purpose, the USA PATRIOT Act amended subsection (a) to require a warrant “by a court with jurisdiction over the offense under investigation or an equivalent state

PATRIOT ACT § 212 (2001), *available at*

<http://www.cdt.org/security/usapatriot/011210crs.pdf> (last visited Aug. 30, 2002) (quoting H.R. REP. NO. 107-236M PT. 1, at 58 (2001)) [hereinafter “TERRORISM”].

121. *Id.* (quoting H.R. REP. NO. 107-236M PT. 1, at 58 (2001)).

122. *Id.* (quoting H.R. REP. NO. 107-236M PT. 1, at 58 (2001)).

123. 18 U.S.C. § 2703 (2000).

124. *Id.* at (a).

125. *Id.*

126. FED. R. CRIM. P. 41(a) advisory committee’s note to 1990 amendment.

127. CRS REPORT FOR CONGRESS, *supra* note 26, at 7 n.14 (quoting *DoJ, supra* note 33, at 55).

128. United States Department of Justice, *supra* note 35.

warrant.”¹²⁹ As a result, the amendment “eliminates the jurisdictional restrictions on access to the content of stored e-mail pursuant to a court order.”¹³⁰ Before the amendment, “only a federal court in the district in which the e-mail was stored could issue the order.”¹³¹ Now, however, “federal courts in the district where an offense under investigation occurred may issue orders applicable ‘without geographic limitation’”¹³² This does not promote warrant-friendly judge shopping because the issuing court must have jurisdiction based on where the crime occurred.¹³³

An example of a jurisdictional problem that might arise is “when an investigator in Boston is seeking electronic mail in the Yahoo! account of a suspected terrorist, he may need to coordinate with agents, prosecutors, and judges in the Northern District of California, none of whom have any other involvement in the investigation.”¹³⁴ In cases involving kidnappings, or an immediate threat to public safety, this hinders law enforcement’s ability to act quickly.¹³⁵ Subsection (a), therefore, furthers public safety by authorizing “courts with jurisdiction over investigations to compel evidence directly, without requiring the intervention of their counterparts in other districts where major Internet service providers are located.”¹³⁶ This is necessary because of the ease of moving about the country and the ease of accessing the Internet. For example, cellular telephones can be purchased with the option of an Internet connection.¹³⁷

Next, section 2703 states that a provider must disclose the contents of an electronic or wire communication, without notice to the customer, if the governmental agency obtains a proper warrant.¹³⁸ A provider must also disclose information when the

129. 18 U.S.C. § 2703(a) (2000), *amended by* USA PATRIOT Act § 220(a)(1), 115 Stat. 272, 291-92.

130. CRS REPORT FOR CONGRESS, *supra* note 26, at 6.

131. *Id.* at 7.

132. *Id.* (quoting 18 U.S.C. § 2703).

133. *DoJ*, *supra* note 33, at 37 (statement of Michael Chertoff, Assistant Attorney General in the Justice Department for the Criminal Division).

134. *Id.* at 55.

135. *Id.*

136. *Id.*

137. See *Nokia Expands Internet Traffic Management Offerings and Lowers Cost of Entry with High-Performance Solutions*, at http://press.nokia.com/PR/200210/879416_5.html (Oct. 30, 2002).

138. 18 U.S.C. § 2703(b)(1)(A).

governmental agency uses an administrative subpoena¹³⁹ or a court order.¹⁴⁰

Once again, in support of his objective to catch terrorists, Attorney General Ashcroft stated:

[t]errorists are trained to change cell phones frequently, to route email through different Internet computers in order to defeat surveillance. Our proposal creates a more efficient technology neutral standard for intelligence gathering, ensuring that law enforcement's ability to trace the communications of terrorists over cell phones, computer networks and the new technologies that may be developed in the years ahead. These changes would streamline intelligence-gathering procedures only. We do not seek changes in the underlying protections in the law for the privacy of law-abiding citizens. The information captured by the proposed technology-neutral standard would be limited to the kind of information you might find in a phone bill, such as the phone numbers dialed by a particular telephone. The content of these communications in this setting would remain off-limits to monitoring by intelligence authorities, except under the current legal standards where content is available under the law which we now use.¹⁴¹

According to amendments made by the USA PATRIOT Act, government agencies can gain information such as the subscriber's name,¹⁴² address,¹⁴³ telephone number,¹⁴⁴ service information,¹⁴⁵ subscriber number,¹⁴⁶ and source of payment (including any credit card or bank account number).¹⁴⁷ The agency needs only an administrative subpoena to gather such information.¹⁴⁸

139. *Id.* at (b)(1)(B)(i).

140. *Id.* at (b)(1)(B)(ii).

141. United States Department of Justice, *supra* note 35.

142. 18 U.S.C. § 2703 (c)(2)(A), *amended by* USA PATRIOT Act § 210(1), 115 Stat. 272, 283.

143. *Id.* at (c)(2)(B), *amended by* USA PATRIOT Act § 210(1), 115 Stat. 272, 283.

144. *Id.* at (c)(2)(C), *amended by* USA PATRIOT Act § 210(1), 115 Stat. 272, 283.

145. *Id.* at (c)(2)(D), *amended by* USA PATRIOT Act § 210(1), 115 Stat. 272, 283.

146. *Id.* at (c)(2)(E), *amended by* USA PATRIOT Act § 210(1), 115 Stat. 272, 283.

147. *Id.* at (c)(2)(F), *amended by* USA PATRIOT Act § 210(1), 115 Stat. 272, 283.

148. *Id.* at (c)(2).

Before the USA PATRIOT Act amendment, investigators could not obtain such records as credit card or bank account numbers, even with a subpoena.¹⁴⁹ This was a problem because “[i]n many cases, users register with Internet service providers using false names, making the form of payment critical to determining the user’s true identity”¹⁵⁰ In fast-moving investigations, identifying the conspirators through Internet communications is critical.¹⁵¹ Billing and other information can identify both the perpetrators and their conspirators and give valuable information about financial accounts.¹⁵²

3. 18 U.S.C. § 2511

Under section 2511,¹⁵³ any person who intentionally intercepts any wire, oral, or electronic communication¹⁵⁴ can be imprisoned or fined.¹⁵⁵ A person cannot intentionally use¹⁵⁶ or disclose to any other person the contents of any communication obtained through prohibited interception techniques.¹⁵⁷

The ECPA permits an officer, acting in the normal course of his employment, to intercept an electronic communication and to disclose or use the information obtained from the communication.¹⁵⁸ The law also permits an officer to intercept an electronic communication if one of the parties consented to the interception.¹⁵⁹ An officer, in the normal course of his official duty, can conduct electronic surveillance.¹⁶⁰

149. See CRS REPORT FOR CONGRESS, *supra* note 26, at 6 n.13 (quoting *Doj*, *supra* note 33, at 55, § 107).

150. *Id.*

151. *Id.*

152. *Id.*

153. 18 U.S.C. § 2511 (2000).

154. *Id.* at (1)(a).

155. *Id.* at (4)(a).

156. *Id.* at (1)(d).

157. *Id.* at (1)(c).

158. *Id.* at (2)(b).

159. *Id.* at (2)(c).

160. *Id.* at (2)(e). “Electronic surveillance” means:

(1) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes;

The USA PATRIOT Act amended this section to make it lawful for an officer to intercept a computer trespasser's¹⁶¹ wire or electronic communication transmitted to or through a protected computer.¹⁶² The officer is permitted to intercept the communication if: (1) the owner of the protected computer authorized the interception;¹⁶³ (2) the officer is lawfully engaged in an investigation;¹⁶⁴ (3) the officer has a reasonable belief that the communication will be relevant to the investigation;¹⁶⁵ and (4) the interception does not acquire communications other than those transmitted to or from the computer trespasser.¹⁶⁶

The purpose of this amendment is to give the victims of

(2) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States, but does not include the acquisition of those communications of computer trespassers that would be permissible under section 2511(2)(i) of Title 18;

(3) the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States; or

(4) the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.

50 U.S.C. § 1801(f).

161. 18 U.S.C. § 2510(21), *amended by USA PATRIOT Act § 217(1)(C)*, 115 Stat. 272, 291 (defining "computer trespasser" as "a person who accesses a protected computer without authorization and thus has no reasonable expectation of privacy in any communication transmitted to, through, or from the protected computer" but does not include "a person known by the owner or operator of the protected computer to have an existing contractual relationship with the owner or operator of the protected computer for access to all or part of the protected computer").

162. 18 U.S.C. § 2511(2)(i), *amended by USA PATRIOT Act § 217(2)*, 115 Stat. 272, 291.

163. *Id.* at (2)(i)(I), *amended by USA PATRIOT Act § 217(2)*, 115 Stat. 272, 291.

164. *Id.* at (2)(i)(II), *amended by USA PATRIOT Act § 217(2)*, 115 Stat. 272, 291.

165. *Id.* at (2)(i)(III), *amended by USA PATRIOT Act § 217(2)*, 115 Stat. 272, 291.

166. *Id.* at (2)(i)(IV), *amended by USA PATRIOT Act § 217(2)*, 115 Stat. 272, 291.

computer trespassers the right to authorize law enforcement to intercept the trespassers' communication.¹⁶⁷ Cyber-attacks "cost companies and citizens millions of dollars and endanger public safety."¹⁶⁸ For example, when a cracker attacks a computer system to disable it, the attack can shut down businesses, emergency responders, or security centers.¹⁶⁹ The attack can cause the target's server "to run out of memory and become incapable of responding to the queries of legitimate customers or users."¹⁷⁰ This creates problems and the victims of such attacks should be able to call upon law enforcement agencies to help them.

4. 18 U.S.C. § 2517

This section provides for the authorization, disclosure, and use of intercepted wire, oral, or electronic communication.¹⁷¹ Specifically, it permits any officer who has lawfully obtained knowledge of the contents of any communication to disclose the contents to another officer to the extent that the disclosure is appropriate to the official duties of each officer.¹⁷² Furthermore, these officers may disclose the information while giving testimony under oath or affirmation in any proceeding.¹⁷³ If an officer intercepts any communication relating to an offense that is not specified in the order of approval, the contents of the communication and the evidence derived from it may be disclosed or used.¹⁷⁴ The officer may also disclose such information in testimony if a judge declares that the contents were otherwise properly intercepted.¹⁷⁵

The USA PATRIOT Act authorizes an officer to share any information gathered about foreign intelligence with the appropriate federal agency.¹⁷⁶ Therefore, "the left hand has to know what the right hand is doing."¹⁷⁷ Before

167. TERRORISM, *supra* note 120, at § 217.

168. *Id.*

169. *Id.*

170. *Id.*

171. 18 U.S.C. § 2517 (2000).

172. *Id.* at (1).

173. *Id.* at (3).

174. *Id.* at (5).

175. *Id.*

176. *Id.* at (6), amended by USA PATRIOT Act § 203(b)(1), 115 Stat. 272, 280.

177. *Doj*, *supra* note 33, at 17 (statement of Larry D. Thompson, Deputy Attorney General of the United States).

the amendment, courts had interpreted the law so that there could be no information sharing.¹⁷⁸ Enforcement agencies faced situations in which the FBI had information, but the law prohibited it from sharing the information with people who could arrest the wrongdoers.¹⁷⁹ Now, such information may be disclosed in cases of official duties only.¹⁸⁰ Perhaps this is a step toward protecting citizens against information leaks.¹⁸¹

5. 18 U.S.C. § 3123

Section 3123¹⁸² concerns the issuance of an order for a pen register¹⁸³ or a trap and trace device.¹⁸⁴ Prior to amendment by the USA PATRIOT Act, this section stated that a court shall enter an ex parte order authorizing the installation and use of a pen register or

178. *DoJ, supra* note 33, at 35 (statement of Michael Chertoff, Assistant Attorney General in the Justice Department for the Criminal Division).

179. *Id.*

180. 18 U.S.C. § 2517(6), *amended by* USA PATRIOT Act § 203(b)(1), 115 Stat. 272, 280.

181. Abuse of information gathering and information sharing is of paramount concern. Congressman Frank noted that “one of the problems we’ve seen historically is the inappropriate release of information garnered by surveillance” *DoJ, supra* note 33, at 27 (statement of Mass. Rep. Barney Frank, Member, House Comm. on the Judiciary).

182. 18 U.S.C. § 3123 (2000).

183. The USA PATRIOT Act also amended the definition of the term “pen register.” As amended, “pen register” is defined as:

[A] device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication, but such term does not include any device or process used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device or process used by a provider or customer or a wire communication service for cost accounting or other like purposes in the ordinary course of its business.

18 U.S.C. § 3127(3), *amended by* USA PATRIOT Act § 216(c)(2), 115 Stat. 272, 290.

184. The USA PATRIOT Act also amended the definition of the term “trap and trace device.” As amended, the term “trap and trace device” is defined as:

[A] device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication.

18 U.S.C. § 3127(4), *amended by* USA PATRIOT Act § 216(c)(3), 115 Stat. 272, 290.

a trap and trace device within the jurisdiction of the court if the court finds that the obtainable information is relevant to an ongoing criminal investigation.¹⁸⁵

The USA PATRIOT Act amends subsection (a) by changing “within the jurisdiction of the court”¹⁸⁶ to “anywhere within the United States.”¹⁸⁷ This gives nation wide effect to pen registers and trap and trace devices.¹⁸⁸ This is important because prior to the amendment, law enforcement officers tracking down criminals wasted time and resources to obtain orders in each jurisdiction.¹⁸⁹ In other words, the amendment eliminates “the need to intrude upon the resources of courts and prosecutors with no connection to the investigation.”¹⁹⁰

The amendment adds that the court order applies to any wire or electronic communication service provider in the United States that can assist in the execution of the order.¹⁹¹ This language permits governmental agencies to trace Internet and computer network communications through multiple service providers.¹⁹² Moreover, when law enforcement serves an order on a person not specifically named in the order, the acting attorney must provide certification that the order applies to a person not listed on the order but being served.¹⁹³ This means that law enforcement officers can issue the order to any Internet service provider who they believe has relevant information.¹⁹⁴

The USA PATRIOT Act also added sub-subsection (a)(3), which demands that an agency that implements an order by using its own pen register or trap and trace device on a packet-switched data network of a provider of electronic communication service to the public maintain a record identifying: (1) any officers who

185. 18 U.S.C. § 3123(a).

186. *Id.*

187. 18 U.S.C. § 3123(a)(1), *amended by* USA PATRIOT Act § 216(b)(1), 115 Stat. 272, 288-89.

188. Lori A. Schechter & Sarah H. Phan, *Privacy on the Internet: Statutory Authority, Enforcement and Policy*, 710 PRACTICING L. INST. 209, 222 (2002).

189. *See* CRS REPORT FOR CONGRESS, *supra* note 26, at 6 n.12 (quoting *Dof, supra* note 33, at 54, § 101).

190. TERRORISM, *supra* note 120, at § 216.

191. 18 U.S.C. § 3123(a)(1), *amended by* USA PATRIOT Act § 216(b)(1), 115 Stat. 272, 288-89.

192. *See* Schechter & Phan, *supra* note 188, at 222.

193. 18 U.S.C. § 3123(a)(1), *amended by* USA PATRIOT Act § 216(b)(1), 115 Stat. 272, 288-89.

194. *See* Osher, *supra* note 22, at 526.

installed or accessed the device to obtain information from the network;¹⁹⁵ (2) the date and time the device was installed and uninstalled, and the duration of each time the device was accessed;¹⁹⁶ (3) the configuration of the device at the time of installation, plus any later modification;¹⁹⁷ and (4) any information that the device has collected.¹⁹⁸ This sub-subsection encourages agencies to set the pen register or trap and trace device to record data electronically.¹⁹⁹ The agency must provide the court that entered the order with the record of the use of the device.²⁰⁰

This amendment refers to a monitoring device, such as Carnivore, that is installed on a public provider's computer.²⁰¹ Carnivore is a software program that was created by the FBI.²⁰² It functions as a cyber-wiretap and is designed to capture network traffic and save that traffic to a storage medium.²⁰³ Carnivore collects two kinds of data: addressing information²⁰⁴ and full content²⁰⁵ of communications.²⁰⁶ This section of the ECPA authorizes the use of the pen mode, which collects addressing information associated with Internet activity.²⁰⁷ In pen mode, "the

195. 18 U.S.C. § 3123(a)(3)(A)(i), *amended by* USA PATRIOT Act § 216(b)(1), 115 Stat. 272, 289.

196. *Id.* at (a)(3)(A)(ii), *amended by* USA PATRIOT Act § 216(b)(1), 115 Stat. 272, 289.

197. *Id.* at (a)(3)(A)(iii), *amended by* USA PATRIOT Act § 216(b)(1), 115 Stat. 272, 289.

198. *Id.* at (a)(3)(A)(iv), *amended by* USA PATRIOT Act § 216(b)(1), 115 Stat. 272, 289.

199. *Id.* at (a)(3)(A), *amended by* USA PATRIOT Act § 216(b)(1), 115 Stat. 272, 289.

200. *Id.* at (a)(3)(B), *amended by* USA PATRIOT Act § 216(b)(1), 115 Stat. 272, 289.

201. *See* Schechter & Phan, *supra* note 188, at 222.

202. *See* McCarthy, *supra* note 9, at 828.

203. *Id.*

204. *Id.* at 834. Carnivore collects addressing information per 18 U.S.C. §§ 3121-27. *Id.* Addressing information is collected in the "pen mode" which suggests that "the FBI believes that obtaining addressing information is essentially the same as obtaining phone numbers via a pen register." *Id.* at 835.

205. *Id.* at 834. Carnivore collects full content per 18 U.S.C. §§ 2510-22. *Id.* Full content information is collected in the "full mode" in which "the FBI can obtain the actual content of real-time communications." *Id.* at 835. The line between content and non-content information was drawn by the United States Supreme Court in *Smith v. Maryland*, 442 U.S. 735, 741-43 (1979).

206. *See* McCarthy, *supra* note 9, at 834; Geoffrey A. North, Note, *Carnivore in Cyberspace: Extending the Electronic Communications Privacy Act's Framework to Carnivore Surveillance*, 28 RUTGERS COMPUTER & TECH. L.J. 155, 165 (2002).

207. *See* 18 U.S.C. § 3123(a)(3)(A), *amended by* USA PATRIOT Act § 216(b)(1), 115 Stat. 272, 289.

FBI can use Carnivore to obtain ‘the TO and FROM e-mail addresses and the IP addresses of computers involved in File Transfer Protocol (FTP) and Hypertext Transfer Protocol (HTTP) sessions.’”²⁰⁸ Carnivore places the FBI and cyber-criminals on a level playing field by giving the FBI similar investigative techniques and procedures as those available to law enforcement in the telephone context.²⁰⁹

Before the enactment of the USA PATRIOT Act, the order issued was required to specify: (1) the identity of the person to whom the telephone line is leased;²¹⁰ (2) the identity of the person who is the subject of the criminal investigation;²¹¹ (3) the number, the physical location of the telephone line, and the geographic limits of the order;²¹² and (4) the offense to which the information relates.²¹³

This subsection promotes Attorney General Ashcroft’s goal of stopping terrorists by updating the statutes to the current state of technology:

Terrorist organizations have increasingly used technology to facilitate their criminal acts and hide their communications from law enforcement. Intelligence-gathering laws that were written for an era of land-line telephone communications are ill-adapted for use in communications over multiple cell phones and computer networks—communications that are also carried by multiple telecommunications providers located in different jurisdictions.²¹⁴

As amended by the USA PATRIOT Act, this subsection includes language that indicates modes of technology beyond

208. See McCarthy, *supra* note 9, at 835 (citing IIT RESEARCH INSTITUTE, INDEPENDENT TECHNICAL REVIEW OF THE CARNIVORE SYSTEM, DRAFT REPORT, at ix (Nov. 17, 2000), available at http://www.usdoj.gov/jmd/publications/carnivore_draft_1.pdf).

209. *Id.* at 844; see North, *supra* note 206, at 166-68; but see Peter J. Georgiton, *The FBI’s Carnivore: How Federal Agents May Be Viewing Your Personal E-Mail and Why There Is Nothing You Can Do About It*, 62 OHIO ST. L.J. 1831, 1866 (noting that “[t]he problems with Carnivore are clear: There are too many possibilities that Carnivore will intercept more e-mail than necessary, too few protections imposed by federal constitutional and statutory law, and an outright absence of sufficient judicial supervision of the FBI”).

210. 18 U.S.C. § 3123(b)(1)(A).

211. *Id.* at (b)(1)(B).

212. *Id.* at (b)(1)(C).

213. *Id.* at (b)(1)(D).

214. United States Department of Justice, *supra* note 35.

telephones. Examples of such language include “the telephone line *or other facility*”²¹⁵ and “the attributes of the communication to which the order applies, including the number *or other identifier* and, if known, the location of the telephone line *or other facility* to which the pen register or trap and trace device is to be attached or applied.”²¹⁶ Such facilities include: “a cellular telephone number; a specific cellular telephone identified by its electronic serial number; an Internet user account or e-mail address; or an Internet protocol address, port number, or similar computer network address or range of addresses.”²¹⁷

6. 18 U.S.C. § 3121

Section 3121 provides an exception to the general prohibition against pen register and trap and trace device use.²¹⁸ Initially, the section states that no person may install or use a pen register or trap and trace device without first obtaining a court order.²¹⁹ The one exception to the general prohibition is in favor of providers of electronic or wire communication.²²⁰ Such providers can use pen registers or trap and trace devices when a user consents to the use²²¹ or when the use relates to the operation, maintenance, and testing of a service or for the protection of the property or rights of the provider.²²² A provider can also use such a device to protect itself, another provider, or a user of the service from fraudulent, unlawful, or abusive use of service.²²³

The next subsection limits a governmental agency which is authorized to use a pen register to the use of technology that restricts the recording or decoding of electronic or other impulses to the dialing and signaling information utilized in the call processing.²²⁴ The USA PATRIOT Act, however, amended the language of this subsection to include a trap and trace device along

215. 18 U.S.C. § 3123(b)(1)(A), *amended by* USA PATRIOT Act § 216(b)(2), 115 Stat. 272, 289 (emphasis added).

216. *Id.* at (b)(1)(C), *amended by* USA PATRIOT Act § 216(b)(2), 115 Stat. 272, 289 (emphasis added).

217. TERRORISM, *supra* note 120.

218. 18 U.S.C. § 3121 (2000).

219. *Id.* at (a).

220. *Id.* at (b).

221. *Id.* at (b)(3).

222. *Id.* at (b)(1).

223. *Id.* at (b)(2).

224. *Id.* at (c).

with the use of a pen register and the use of technology that records or decodes “dialing, routing, addressing, and signaling information utilized in the processing and transmitting of wire or electronic communication so as not to include the contents of any wire or electronic communication.”²²⁵

By adding the words “dialing” and “routing,” this amendment permits a governmental agency to track e-mail and Internet usage.²²⁶ However, it does not allow the collecting of e-mail subject lines.²²⁷ This amendment also permits the use of software like Carnivore.²²⁸

III. CONCLUSION

Computer crime presents new challenges to law enforcement agencies. The most troublesome challenge is that the cyber-world is much larger than any country’s borders.²²⁹ The next challenge is that in computer crime cases officials cannot track a trail of physical evidence as they would to find the burglar who burglarized a home.²³⁰

To give these officials the tools they need to stop cyber-crime, the laws need to change as technology changes.²³¹ The USA

225. 18 U.S.C § 3121(c), amended by USA PATRIOT Act § 216(a), 115 Stat. 272, 288.

226. See McCarthy, *supra* note 9, at 445 (2002); Schecter & Phan, *supra* note 188, at 222; Richard Willing, *Anti-terror Bill Expands Government’s Reach*, USA TODAY, Oct. 25, 2001, at A7.

227. TERRORISM, *supra* note 120, at section 216.

228. See *supra* Part II.C.5 (discussing how Carnivore functions).

229. Shawn P. McCarthy, *If You Want to Catch a Hacker, Hire One—Or be a Sophisticated Fed*, INTERNAUT, available at http://gcn.com/archives/gcn/1998/june1/if_you_want_to_catch_a_hacker.htm (June 1, 1998) (“[C]yberspace knows no boundaries.”).

230. *Cybercrime Enforcement: Hearing on H.R. 3482 Before the Subcomm. On Crime, House Comm. on the Judiciary, 107th Cong.* (2002) (statement of Susan Kelley Koeppen, Corporate Attorney, Microsoft Corp.):

In the online world, we often face a problem with criminal actions that are not treated as crimes, and with criminals who do not do time. While our society does not tolerate people breaking into brick-and-mortar homes and businesses, we inexplicably seem to have more tolerance for computer break-ins. Yet breaking into computers is just as much a crime as breaking into homes and businesses. Both break-ins harm innocent people and weaken American businesses, and computer attacks need to be treated as the truly criminal activities that they most assuredly are.

Id.

231. “We are not asking the law to expand; just to grow as technology grows.

PATRIOT Act provides such tools by eliminating jurisdictional boundaries of courts, permitting Internet service providers to share information with law enforcement agencies, and providing for the use of software like Carnivore. Once tracked down, criminals need to face a deterring penalty for their actions. Cyber-crime needs to be prevented because individuals, the government, and industry use computers and the Internet to communicate and gather information, to market goods, to solicit and consummate business deals, and to store sensitive data.

This information has historically been available when criminals used pre-digital technologies. This same information should be available to law enforcement officials today.” United States Department of Justice, *supra* note 35. “[N]one of [these provisions] is a revolution in the law. All of these are techniques and principles that we have been applying for 20 or 30 years in some context. We are simply trying to apply them across the board so we don’t have gaps in the coverage.” *Dof, supra* note 33, at 28 (statement of Michael Chertoff, Assistant Attorney General in the Justice Department for the Criminal Division).