Gary Kurtz, SBN 128295
Law Office of Gary Kurtz
A Professional Law Corporation
20335 Ventura Boulevards
Suite 200
Woodland Hills, California 91364

Telephone: 818-884-8400
Telefax 818-884-8404

Attorneys for Plaintiff
Pallorium, Inc.

SUPERIOR COURT OF THE STATE OF CALIFORNIA

FOR THE COUNTY OF ORANGE

Pallorium, Inc., Plaintiff, vs. Stephen J. Jared, etc., Defendants.	Case No.: 03CC12794 Assigned to: Hon. Geoffrey T. Glass PLAINTIFF'S OBJECTIONS TO TENTITIVE RULING OF TRIAL COURT Dept.: C-22

I. Introduction

The trial court bifurcated the trial of this matter so that defendant's immunity defense was tried first. Testimony and arguments were presented and received with respect to the scope and applicability of a federal immunity defense. On July 13, 2005, the Court issued and mailed its tentative decision. Pallorium objects to the tentative decision and the ruling.

Pursuant to Rule 232(e), California Rules of Court, plaintiff objects to the ruling on the following grounds:

1. Even if we were to assume that the Court is correct with respect to all of its analysis, the ruling unconstitutionally violates Pallorium's right to a jury trial on the issue of whether defendant was acting in good faith.

2. Defendant's conduct, as testified to by defendant, cannot **as a matter of law,** be held to be in good faith because it violates federal criminal statutes.

3. The Court erred in its application of the immunity statute to the situation at bar.

II. Objection To Tentative Decision

Defendant was sued for careless and arrogant efforts to obstruct Internet communications. He blundered by including Pallorium's e-mail server on his block lists, and then he failed and refused to remove Pallorium, as he commonly refused to remove others. Defendant's conduct was intentional, reckless **and criminal**, resulting in substantial damages to Pallorium and others.

The issue before this Court was an affirmative defense based on the Communications Decency Act ("CDA") 47 U.S.C. § 230, which reads in relevant part as follows.

> (1) Treatment of publisher or speaker - No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.
> (2) Civil liability - No provider or user of an interactive computer service shall be held liable on account of -

> (A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or
>
> (B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1). [1] (A)."

The court has ruled for Pallorium on the (1) provision, so that will not be discussed.

A. The Tentative Denies Pallorium's Right To Jury Trial

Pallorium preserved its right to a jury trial. A jury trial was initially requested, fees were posted, and jury instructions were lodged at the M.S.C. This Court even commented at the first trial stage that a jury would be summoned, depending on the immunity defense.

The Court's tentative decision improperly denies Pallorium's jury right by deciding that defendant was acting in good faith. That is not a determination of law as to whether the immunity defense could be presented to the jury, which is all the Court could do. That determination went beyond the proper role of the court and invaded Pallorium's right to a jury determination.

"The California Constitution . . . set out the right to a jury trial in the strongest possible terms." Because Pallorium pleaded causes of action were legal, not equitable, seeking damages, it had a right to a jury. *See Raedeke v. Gibralter Savings & Loan Ass'n*, 10 Cal.3d 665, 672 (1974). In *Gemini Aluminum Corp. v. California Custom Shapes, Inc.*, 95 Cal.App.4th 1249 (2002), the court resolved issues regarding the allocation of a burden of proof in jury instructions regarding an affirmative defense. Although the decisional authorities generally deal with affirmative defenses in criminal cases, the right to a jury clearly includes the resolution of affirmative defenses. *See People v. Frazier*, 128 Cal.App.4th 807 (2005); *People v. Neidinger*, 127 Cal.App.4th 1120 (2005).

In the instant case, assuming, arguendo, the validity of the Court's tentative analysis, the immunity issue should have been presented to the jury. The court could go so far as determining that defendant presented sufficient evidence so that there was legal basis for a jury trial on whether defendant was entitled to immunity. A jury instruction should have been drafted to tell the jury that they should find defendant immune from liability if they find that defendant (1) was acting in good faith and (2) acted to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable.

"[T]he improper denial of the right to jury is reversible error per se." *Grafton Partners LP v. Superior Court*, 115 Cal.App.4th 700, 705 (2004). This Court still has the opportunity to avoid being reversed for depriving Pallorium of its jury right.

B. As A Matter Of Law, Defendant Can Not Be Found To Have Acted In Good Faith Because His Conduct Was Criminal

47 U.S.C. § 230(2)(A) requires that the proponent of the defense demonstrate that his actions were in good faith. Obviously, criminal activity cannot be in "good faith". *See Chavers v. Gatke Corp.*, 107 Cal.App.4th 606, 612 (2003). There can be no finding of good faith in this case.

1. Defendant's Criminal Acts Cannot Be Good Faith

Defendant has testified to violating the terms of 18 U.S.C. § 1030(a)(5)(A). That statute imposes criminal penalties on anyone who:

> **(i)** knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;
> **(ii)** intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or
> **(iii)** intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage; and

The code section continues to define "protected computer" to include any computer "which is used in interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States." 18 U.S.C. § 1030(e)(2)(B).

The UCLA Journal of Law and Technology published an article on this statute, which ironically was directed to prevent DDOS attacks. A copy of the article is attached hereto. The authors reframe the language of the statute to set forth the following elements:

> Title 18 U.S.C. § 1030(5)(B) was essentially crafted to mimic Section A of Title 18 U.S.C. § 1030(5). However, Section B requires a lower standard of knowledge to invoke a violation. It states:
>
> "through means of a computer used in interstate commerce or communication, knowingly causes the transmission of a program, information, code, or command to a computer or computer system -
> (I) with reckless disregard of a substantial and unjustifiable risk that the transmission will -
> (I) damage, or cause damage to, a computer, computer system, network, information, data or program; or
> (II) withhold or deny or cause the withholding or denial of the use of a computer, computer services, system, network, information, data, or program.

Defendant in this case was proud to have **criminally** created a program and code that denied use of computers, computer systems and networks of third parties, including Pallorium. Further, defendant admitted a criminal violation of this federal statute. Pallorium's computer mail server was a "protected computer" because it was used to do interstate and foreign commerce and communications. Defendant violated each and every subsection quoted infra:

- Defendant knowingly caused the transmission of an e-mail (information) to test whether Pallorium had an open server with the intent to block e-mails (causing damage) if there was a positive response to the test. [violating (A)(i)]

- Defendant intentionally accessed Pallorium's e-mail server without authorization and got a false positive response indicating it was an open server. He then recklessly caused damage by blocking e-mail without an effective way to remove the IP addresses from defendant's black lists. [violating (A)(ii)]

- Defendant intentionally accessed Pallorium's e-mail server and, as a result, received a false positive response indicating it was an open server, which resulted in damage because Pallorium's e-mail was blocked. [violating (A)(iii)]

2. Immunizing Defendant's Conduct Would Be Dangerous

This Court's tentative ruling immunizing defendant's conduct (which obstructed legitimate third party e-mail and Internet use based on his personal code of conduct) would create a horrible expansion of existing precedent. It should not be surprising that neither party has found any "on point" decisional authorities, as the immunization of content-neutral communications obstructions is well beyond the intent and language of the statute. This Court is saying that any person who has an honest subjective belief that he is doing good is immune from conduct that obstructs Internet communication from third parties. Examples of horrific applications abound, and the following are some of the more obvious illustrations:

- Would this Court immunize the conduct of the Society for Historical Review (or some other Neo-Nazi organization) if it decided to block the e-mail of the Simon Wiesenthal Center?

- Would this Court immunize the conduct of the North American Man-Boy Love Association (or some other pedophile society) if it decided to block the e-mail of the National Center for Missing and Exploited Children?

- Would this Court immunize the conduct of Al Qaida if it decided to block the e-mail of the C.I.A.?

These examples are extreme, but no more extreme than defendant's conduct. In an ultimate example of bad faith, when defendant decided to end is e-mail obstruction hobby, he published code **<u>that blocked the world</u>**. When he did this, for some period of time, all e-mail that went through is major clients (such as Prodigy, Ameritech and SBC) would not be delivered to the Simon Wiesenthal Center, the National Center for Missing and Exploited Children, the C.I.A., or anyone else. The Communications Decency Act **was not** designed to apply to people intentionally disrupting Internet use. Defendant's conduct in this case had the same effect as the DDOS attack he complains about, and it was not privileged.

3. <u>Defendant's Conduct Was NOT In Good Faith</u>

The definition of "good faith" commonly requires honesty in fact, as well as reasonable and fair conduct. It is often interpreted based on an objective standard. *See Brashers Cascade Auto Auction v. Valley Auto Sales and Leasing*, 119 Cal.App.4th 1038 (2004); *Bardis v. Oates*, 119 Cal.App.4th 1 (2004). In *State Farm Mutual Ins. Co v. Superior Court*, 114 Cal.App.4th 434, 453 (2003), the court explained: "The doctrine of good faith then requires the party vested with contractual discretion to exercise that discretion reasonably and with proper motive, not arbitrarily, capriciously, or in a manner inconsistent with the reasonable expectations of the parties." [citation omitted.] A key element is "honesty of purpose." *Id.* at 450.

This Court seems to be treating defendant as some Internet Robin Hood who protected innocent users from the bane of SPAM. In fact, defendant has a history of institutionalization for mental illness, domestic abuse problems, a criminal assault on a law enforcement officer, and substance abuse. He was a substance abuser when he published is blacklists and, most likely, did not appropriately respond to complaints because he was impaired. The "cleaned up" witness at trial was not true picture of the person who intentionally attempted blocked e-mail worldwide.

Defendant certainly did not conduct himself in good faith with respect to Pallorium. All he had to do was shut off his system or remove Pallorium from his list, and the problems would have been mitigated to a trivial level. To do so, he would have had to travel back to California from Memphis to get into his system. This would have been prudent and in good faith, independent of Pallorium's problems, because all of defendant's safeguards had been disabled by a DDOS attack. Defendant could not be bothered to return to California to fix or shut down his system. Instead, he said he fretted unproductively in Memphis.

Pallorium was improperly listed, and that listing obstructed considerable legitimate business. Mr. Rambam used every fail safe on defendant's system. He used the internal complaint method. He sent e-mails. He sent telefaxes. He called defendant. Defendant's response was to do nothing to help or remove Pallorium from his blacklist. Instead, defendant said "fuck-you", hung up on Mr. Rambam and did nothing to solve the problem. This was no uncommon, as defendant had incorrectly listed many others and had refused to correct the listing when alerted of his mistakes. Those were **not** the acts of a man conducting himself in good faith. That was **not** the conduct of a man deserving of federal immunity for "good faith" conduct.

Finally, it is worthy of repeating that at the end of his "hobby" defendant decided to block the world rather than simply turning off his computer. He is a bad man who did bad things and should not be protected by a statute that has a good faith standard.

C. Defendant Does Not Qualify For Protection

The 47 U.S.C. § 230(2)(A) and (B) immunity only apply to a provider or user of an "interactive computer service". 47 U.S.C. § 230(f)(2) defines that term as follows:

> The term "interactive computer service" means any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions.

Defendant clearly and obviously does not satisfy most of the standards set forth in the statute.

Defendant testified that he did two things relevant to this action. First, defendant created an e-mail program that sent e-mails to other servers, attempted to hijack them to see if they are open, and reported the results in the form of a list of open servers. Second, defendant posted the list and amended list on his web page for the world to freely see and use. If these events qualify for immunity, then every user of the Internet would qualify for the immunity. Any definition that would include defendant would not merely be liberal and broad; it would be unlimited.

Batzel v. Smith, 333 F.3d 1018 (9th Cir. 2003), cited by defendant with approval, is instructive on the point. The majority opinion made it clear that congress intended the immunity to apply to specified, somewhat narrow, services and users of those services:

> Supplying a "provider or user of an interactive computer service" with immunity in such circumstances is not consistent with Congress's expressly stated purposes in adopting § 230. Free speech and the development of the Internet are not "promote[d]" by affording immunity when providers and users of "interactive computer service[s]" knew or had reason to know that the information provided was not intended for publication on the Internet. Quite the contrary: Users of the Internet are likely to be discouraged from sending e-mails for fear that their e-mails may be published on the web without their permission.
>
> **Such a scenario is very different from the bulletin boards that Congress had in mind when passing § 230.**

Id. at 1033-34. (Emphasis supplied). The partially concurring and dissenting opinion provides additional helpful analysis:

> My interpretation of § 230 is consistent with the CDA's legislative history. Congress understood that entities that facilitate communication on the Internet--particularly entities that operate e-mail networks, "chat rooms," "bulletin boards," and "listservs"--have special needs. The amount of information communicated through such services is staggering. Millions of communications are sent daily. It would be impossible to screen all such communications for libelous or offensive content.

Id. at 1039. Footnote 15 summarizes relevant authorities, as follows:

> Other courts construing § 230(f)(2) have recognized that the definition includes a wide range of cyberspace services, not only internet service providers. *See, e.g., Gentry v. eBay, Inc.*, 99 Cal.App.4th 816, 831 & n. 7, 121 Cal.Rptr.2d 703 (2002) (on-line auction website is an "interactive computer service"); *Schneider v. Amazon.com*, 108 Wash.App. 454, 31 P.3d 37, 40-41 (2001) (on-line bookstore Amazon.com is an "interactive computer service"); *Barrett v. Clark*, 2001 WL 881259 at *9 (Cal.Sup.Ct.2001) (newsgroup considered an "interactive computer service"); *see also Ben Ezra*, 206 F.3d at 985 (parties conceded that AOL was an interactive computer service when it published an on-line stock quotation service); *Zeran*, 129 F.3d at 330 (AOL assumed to be interactive computer service when it operated bulletin board service for subscribers); *Blumenthal*, 992 F.Supp. at 49-50 (parties conceded that AOL was an "interactive computer service" even when it functioned as the publisher of an on-line gossip column).

None of the authorities cited to this Court, or found by plaintiff, has applied immunity to some deranged misanthrope sending e-mails and publishing lists of IP addresses from his home computer.

This court errs when concluding that defendant was a provider of an "interactive computer service". He had home computers, and there was no testimony that he provided them for use by anyone else in the relevant time frame. Rather, he provided lists of IP addresses to anyone who connected to his web page. The third parties would then take the lists and use them independent of defendant. At most, defendant provided information for use by others, not an information service that enabled access to a computer server.

D. Defendant's Block Lists Are Not Content Based, So He Cannot Claim Immunity Pursuant To 47 U.S.C. § 230(c)(2)

Section (2) only applies to material that the "user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable." Defendant does not block e-mail on the basis of content. He does not block because he considers the content of e-mails to be "be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable." He blocks based on the configuration of an e-mail server, which does not qualify for protection.

This Court errs when it expands the immunity to content-neutral communications. This Court's application of the statute fails to give meaning to the word "material". The material must "be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable." That means content – not simply the fact that the e-mails were unsolicited or, in this case, were transmitted through an open e-mail server. It is not the "material" that Jared found offensive or objectionable, and he did not filter based on material he believed to "be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable." Accordingly, defendant's content neutral filtering does not fit within the statutory language.

E. Defendant's Block Lists Are Not Immune Pursuant To 47 U.S.C. § 230(c)(3)

Section (3) also fails based on the word "material". Even if we assume the validity of the Court's analysis, defendant did not provide the "technical means to restrict access to material." At most, defendant provided the technical means to restrict access to IP addresses, no matter what material was being communicated.

Dated: July 25, 2005

Law Office of Gary Kurtz, A P.L.C.

By:
Gary Kurtz Esq., Attorneys for Plaintiff
Pallorium, Inc.

United States Statutes

Title 18. Crimes and Criminal Procedure

Part I. CRIMES

Chapter 47. FRAUD AND FALSE STATEMENTS

Current through January 6, 2003

§ 1030. Fraud and related activity in connection with computers.

(a) Whoever-

(1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains-

(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602 (n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

(B) information from any department or agency of the United States; or

(C) information from any protected computer if the conduct involved an interstate or foreign communication;

(3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States;

4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period;

5)

A)

i) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes amage without authorization, to a protected computer;

ii) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

iii) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage; and

B) by conduct described in clause (i), (ii), or (iii) of subparagraph (A), caused (or, in the case of an attempted offense, would, if completed, ave caused)-

) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the nited States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in alue;

i) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or ore individuals;

ii) physical injury to any person;

v) a threat to public health or safety; or

) damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security;

(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if-

(A) such trafficking affects interstate or foreign commerce; or

(B) such computer is used by or for the Government of the United States; [1]

(7) with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to cause damage to a protected computer;

shall be punished as provided in subsection (c) of this section.

(b) Whoever attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section.

(c) The punishment for an offense under subsection (a) or (b) of this section is-

(1)

(A) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(1) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than twenty years, or both, in the case of an offense under subsection (a)(1) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(2)

(A) except as provided in subparagraph (B), a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2), (a)(3), (a)(5)(A)(iii), or (a)(6) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(2), or an attempt to commit an offense punishable under this subparagraph, if-

(i) the offense was committed for purposes of commercial advantage or private financial gain;

(ii) 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; or

iii) the value of the information obtained exceeds $5,000; and

C) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2), (a)(3) or (a)(6) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

3)

A) a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(4) or (a)(7) of this ection which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this ubparagraph; and

B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4), (a)(5)(A)(iii), r (a)(7) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable nder this subparagraph;

4)

A) except as provided in paragraph (5), a fine under this title, imprisonment for not more than 10 years, or both, in the case of an offense under ubsection (a)(5)(A)(i), or an attempt to commit an offense punishable under that subsection;

B) a fine under this title, imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(5)(A)(ii), or an attempt commit an offense punishable under that subsection;

C) except as provided in paragraph (5), a fine under this title, imprisonment for not more than 20 years, or both, in the case of an offense under bsection (a)(5)(A)(i) or (a)(5)(A)(ii), or an attempt to commit an offense punishable under either subsection, that occurs after a conviction for another offense under this section; and

(5)

(A) if the offender knowingly or recklessly causes or attempts to cause serious bodily injury from conduct in violation of subsection (a)(5)(A)(i), a fine under this title or imprisonment for not more than 20 years, or both; and

(B) if the offender knowingly or recklessly causes or attempts to cause death from conduct in violation of subsection (a)(5)(A)(i), a fine under this title or imprisonment for any term of years or for life, or both.

(d)

(1) The United States Secret Service shall, in addition to any other agency having such authority, have the authority to investigate offenses under this section.

(2) The Federal Bureau of Investigation shall have primary authority to investigate offenses under subsection (a)(1) for any cases involving espionage, foreign counterintelligence, information protected against unauthorized disclosure for reasons of national defense or foreign relations, or Restricted Data (as that term is defined in section 11y of the Atomic Energy Act of 1954 (42 U.S.C. 2014 (y)), except for offenses affecting the duties of the United States Secret Service pursuant to section 3056 (a) of this title.

(3) Such authority shall be exercised in accordance with an agreement which shall be entered into by the Secretary of the Treasury and the Attorney General.

(e) As used in this section-

(1) the term "computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device;

(2) the term "protected computer" means a computer-

(A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the inancial institution or the Government; or

B) which is used in interstate or foreign commerce or communication, including a computer located outside the United States that is used in a nanner that affects interstate or foreign commerce or communication of the United States;

3) the term "State" includes the District of Columbia, the Commonwealth of Puerto Rico, and any other commonwealth, possession or territory of the United States;

4) the term "financial institution" means-

A) an institution, with deposits insured by the Federal Deposit Insurance Corporation;

B) the Federal Reserve or a member of the Federal Reserve including any Federal Reserve Bank;

C) a credit union with accounts insured by the National Credit Union Administration;

D) a member of the Federal home loan bank system and any home loan bank;

E) any institution of the Farm Credit System under the Farm Credit Act of 1971;

F) a broker-dealer registered with the Securities and Exchange Commission pursuant to section 15 of the Securities Exchange Act of 1934;

G) the Securities Investor Protection Corporation;

I) a branch or agency of a foreign bank (as such terms are defined in paragraphs (1) and (3) of section 1(b) of the International Banking Act of 978); and

) an organization operating under section 25 or section 25(a) [2] of the Federal Reserve Act;

) the term "financial record" means information derived from any record held by a financial institution pertaining to a customer's relationship th the financial institution;

) the term "exceeds authorized access" means to access a computer with authorization and to use such access to obtain or alter information in computer that the accesser is not entitled so to obtain or alter,

(7) the term "department of the United States" means the legislative or judicial branch of the Government or one of the executive departments enumerated in section 101 of title 5;

(8) the term "damage" means any impairment to the integrity or availability of data, a program, a system, or information;

(9) the term "government entity" includes the Government of the United States, any State or political subdivision of the United States, any foreign country, and any state, province, municipality, or other political subdivision of a foreign country;

(10) 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;

(11) the term "loss" means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the 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; and

(12) the term "person" means any individual, firm, corporation, educational institution, financial institution, governmental entity, or legal or other entity.

(f) This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States.

(g) Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in clause (i), (ii), (iii), (iv), or (v) of subsection (a)(5)(B). Damages for a violation involving only conduct described in subsection (a)(5)(B)(i) are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage. No action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware.

(h) The Attorney General and the Secretary of the Treasury shall report to the Congress annually, during the first 3 years following the date of the enactment of this subsection, concerning investigations and prosecutions under subsection (a)(5).

1] So in original. Probably should be followed by "or".

2] See References in Text note below.

Note:

ource

Added Pub. L. 98-473, title II, § 2102(a), Oct. 12, 1984, 98 Stat. 2190; amended Pub. L. 99-474, § 2, Oct. 16, 1986, 100 Stat. 1213; Pub. L. 100-690, title VII, § 7065, lov. 18, 1988, 102 Stat. 4404; Pub. L. 101-73, title IX, § 962(a)(5), Aug. 9, 1989, 103 Stat. 502; Pub. L. 101-647, title XII, § 1205(e), title XXV, § 2597(j), title XXXV, § 533, Nov. 29, 1990, 104 Stat. 4831, 4910, 4925; Pub. L. 103-322, title XXIX, § 290001(b)-(f), Sept. 13, 1994, 108 Stat. 2097-2099; Pub. L. 104-294, title II, § 201, tle VI, § 604(b)(36), Oct. 11, 1996, 110 Stat. 3491, 3508; Pub. L. 107-56, title V, § 506(a), title VIII, § 814(a)-(e), Oct. 26, 2001, 115 Stat. 366, 382-384; Pub. L. 107-73, div. B, title IV, §§ 4002(b)(1), (12), 4005 (a)(3), (d)(3), Nov. 2, 2002, 116 Stat. 1807, 1808, 1812, 1813; Pub. L. 107-296, title II, § 225(g), Nov. 25, 2002, 116 Stat. 158.)

eferences in Text

ection 11 of the Atomic Energy Act of 1954, referred to in subsec. (a)(1), is classified to section 2014 of Title 42, The Public Health and Welfare.

he Fair Credit Reporting Act, referred to in subsec. (a)(2)(A), is title VI of Pub. L. 90-321, as added by Pub. L. 91-508, title VI, § 601, Oct. 26, 1970, 84 Stat. 1127, as mended, which is classified generally to subchapter III (§ 1681 et seq.) of chapter 41 of Title 15, Commerce and Trade. For complete classification of this Act to the ode, see Short Title note set out under section 1601 of Title 15 and Tables.

he Farm Credit Act of 1971, referred to in subsec. (e)(4)(E), is Pub. L. 92-181, Dec. 10, 1971, 85 Stat. 583, as amended, which is classified generally to chapter 23 (§ 001 et seq.) of Title 12, Banks and Banking. For complete classification of this Act to the Code, see Short Title note set out under section 2001 of Title 12 and Tables.

ection 15 of the Securities Exchange Act of 1934, referred to in subsec. (e)(4)(F), is classified to section 78o of Title 15, Commerce and Trade.

ection 1(b) of the International Banking Act of 1978, referred to in subsec. (e)(4)(H), is classified to section 3101 of Title 12, Banks and Banking.

ction 25 of the Federal Reserve Act, referred to in subsec. (e)(4)(I), is classified to subchapter I (§ 601 et seq.) of chapter 6 of Title 12. Section 25(a) of the Federal serve Act, which is classified to subchapter II (§ 611 et seq.) of chapter 6 of Title 12, was renumbered section 25A of that act by Pub. L. 102-242, title I, § 142(e)(2), c. 19, 1991, 105 Stat. 2281.

e date of the enactment of this subsection, referred to in subsec. (h), is the date of enactment of Pub. L. 103-322, which was approved Sept. 13, 1994.

nendments

02-Subsec. (a)(5)(B). Pub. L. 107-273, § 4005(a)(3), realigned margins.

bsec. (c)(2)(B). Pub. L. 107-273, § 4002(b)(1), realigned margins.

Subsec. (c)(2)(B)(iii). Pub. L. 107-273, § 4002(b)(12)(A), inserted "and" at end.

Subsec. (c)(3)(B). Pub. L. 107-273, § 4005(d)(3), inserted comma after "(a)(4)".

Subsec. (c)(4)(A), (C). Pub. L. 107-296, § 225(g)(2), inserted "except as provided in paragraph (5)," before "a fine under this title".

Subsec. (c)(5). Pub. L. 107-296, § 225(g)(1), (3), (4), added par. (5).

Subsec. (e)(4)(I). Pub. L. 107-273, § 4002(b)(12)(B), substituted semicolon for period at end.

2001-Subsec. (a)(5)(A). Pub. L. 107-56, § 814(a)(1)-(3), designated existing provisions as cl. (i), redesignated subpars. (B) and (C) as cls. (ii) and (iii), respectively, of subpar. (A), and inserted "and" at end of cl. (iii).

Subsec. (a)(5)(B). Pub. L. 107-56, § 814(a)(4), added subpar. (B). Former subpar. (B) redesignated cl. (ii) of subpar. (A).

Subsec. (a)(5)(C). Pub. L. 107-56, § 814(a)(2), redesignated subpar. (C) as cl. (iii) of subpar. (A).

Subsec. (a)(7). Pub. L. 107-56, § 814(b), struck out ", firm, association, educational institution, financial institution, government entity, or other legal entity," before "any money or other thing of value".

Subsec. (c)(2)(A). Pub. L. 107-56, § 814(c)(1)(A), inserted "except as provided in subparagraph (B)," before "a fine", substituted "(a)(5)(A)(iii)" for "(a)(5)(C)", and struck out "and" at end.

Subsec. (c)(2)(B). Pub. L. 107-56, § 814(c)(1)(B), inserted "or an attempt to commit an offense punishable under this subparagraph," after "subsection (a)(2)," in introductory provisions.

Subsec. (c)(2)(C). Pub. L. 107-56, § 814(c)(1)(C), struck out "and" at end.

Subsec. (c)(3). Pub. L. 107-56, § 814(c)(2), struck out ", (a)(5)(A), (a)(5)(B)," after "subsection (a)(4)" in subpars. (A) and (B) and substituted "(a)(5)(A)(iii)" for "(a)(5)(C)" in subpar. (B).

Subsec. (c)(4). Pub. L. 107-56, § 814(c)(3), added par. (4).

Subsec. (d). Pub. L. 107-56, § 506(a), amended subsec. (d) generally. Prior to amendment, subsec. (d) read as follows: "The United States Secret Service shall, in addition to any other agency having such authority, have the authority to investigate offenses under subsections (a)(2)(A), (a)(2)(B), (a)(3), (a)(4), (a)(5), and (a)(6) of this section. Such authority of the United States Secret Service shall be exercised in accordance with an agreement which shall be entered into by the Secretary of the Treasury and the Attorney General."

Subsec. (e)(2)(B). Pub. L. 107-56, § 814(d)(1), inserted ", including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States" before semicolon.

Subsec. (e)(7). Pub. L. 107-56, § 814(d)(2), struck out "and" at end.

Subsec. (e)(8). Pub. L. 107-56, § 814(d)(3), added par. (8) and struck out former par. (8) which read as follows: "the term 'damage' means any impairment to the integrity or availability of data, a program, a system, or information, that

"(A) causes loss aggregating at least $5,000 in value during any 1-year period to one or more individuals;

"(B) modifies or impairs, or potentially modifies or impairs, the medical examination, diagnosis, treatment, or care of one or more individuals;

"(C) causes physical injury to any person; or

"(D) threatens public health or safety; and".

ubsec. (e)(10) to (12). Pub. L. 107-56, § 814(d)(4), (5), added pars. (10) to (12).

ubsec. (g). Pub. L. 107-56, § 814(e), substituted "A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in lause (i), (ii), (iii), (iv), or (v) of subsection (a)(5)(B). Damages for a violation involving only conduct described in subsection (a)(5)(B)(i) are limited to economic amages." for "Damages for violations involving damage as defined in subsection (e)(8)(A) are limited to economic damages." and inserted at end "No action may be rought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware."

996-Subsec. (a)(1). Pub. L. 104-294, § 201(1)(A), substituted "having knowingly accessed" for "knowingly accesses", "exceeding authorized access" for "exceeds uthorized access", "such conduct having obtained information" for "such conduct obtains information", and "could be used to the injury of the United States" for "is to e used to the injury of the United States", struck out "the intent or" before "reason to believe", and inserted before semicolon at end "willfully communicates, delivers, ansmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted e same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it".

ubsec. (a)(2). Pub. L. 104-294, § 201(1)(B), inserted dash after "thereby obtains", redesignated remainder of par. (2) as subpar. (A), and added subpars. (B) and (C).

ıbsec. (a)(3). Pub. L. 104-294, § 201(1)(C), inserted "nonpublic" before "computer of a department or agency", struck out "adversely" after "and such conduct", and ıbstituted "that use by or for the Government of the United States" for "the use of the Government's operation of such computer".

ıbsec. (a)(4). Pub. L. 104-294, § 201(1)(D), substituted "protected computer" for "Federal interest computer" and inserted "and the value of such use is not more than 5,000 in any 1-year period" before semicolon at end.

ıbsec. (a)(5). Pub. L. 104-294, § 201(1)(E), inserted par. (5) and struck out former par. (5) which related to fraud in connection with computers in causing transmission of program, information, code, or command to a computer or computer system in interstate or foreign commerce which damages such system, program, information, or code, or causes a withholding or denial of use of hardware or software, or transmits viruses which causes damage in excess of $1,000 or more during any one-year period, or modifies or impairs medical examination, diagnosis, treatment or care of individuals.

Subsec. (a)(5)(B)(ii)(II)(bb). Pub. L. 104-294, § 604(b)(36)(A), which directed insertion of "or" at end of subsec., could not be executed because no subsec. (a)(5)(B)(ii)(II)(bb) existed subsequent to amendment by Pub. L. 104-294, § 201(1)(E). See above.

Subsec. (a)(7). Pub. L. 104-294, § 201(1)(F), added par. (7).

Subsec. (c)(1). Pub. L. 104-294, § 201(2)(A), substituted "under this section" for "under such subsection" in subpars. (A) and (B).

Subsec. (c)(1)(B). Pub. L. 104-294, § 604(b)(36)(B), struck out "and" after semicolon at end.

Subsec. (c)(2)(A). Pub. L. 104-294, § 201(2)(B)(i), inserted ", (a)(5)(C)," after "(a)(3)" and substituted "under this section" for "under such subsection".

Subsec. (c)(2)(B). Pub. L. 104-294, § 201(2)(B)(iii), added subpar. (B). Former subpar. (B) redesignated (C).

Subsec. (c)(2)(C). Pub. L. 104-294, § 201(2)(B)(iv), substituted "under this section" for "under such subsection" and inserted "and" at end.

Pub. L. 104-294, § 201(2)(B)(ii), redesignated subpar. (B) as (C).

Subsec. (c)(3)(A). Pub. L. 104-294, § 201(2)(C)(i), substituted "(a)(4), (a)(5)(A), (a)(5)(B), or (a)(7)" for "(a)(4) or (a)(5)(A)" and "under this section" for "under such subsection".

Subsec. (c)(3)(B). Pub. L. 104-294, § 201(2)(C)(ii), substituted "(a)(4), (a)(5)(A), (a)(5)(B), (a)(5)(C), or (a)(7)" for "(a)(4) or (a)(5)" and "under this section" for "under such subsection".

Subsec. (c)(4). Pub. L. 104-294, § 201(2)(D), struck out par. (4) which read as follows: "a fine under this title or imprisonment for not more than 1 year, or both, in the case of an offense under subsection (a)(5)(B)."

Subsec. (d). Pub. L. 104-294, § 201(3), inserted "subsections (a)(2)(A), (a)(2)(B), (a)(3), (a)(4), (a)(5), and (a)(6) of" before "this section" in first sentence.

Subsec. (e)(2). Pub. L. 104-294, § 201(4)(A)(i), substituted "protected" for "Federal interest" in introductory provisions.

Subsec. (e)(2)(A). Pub. L. 104-294, § 201(4)(A)(ii), substituted "that use by or for the financial institution or the Government" for "the use of the financial institution's operation or the Government's operation of such computer".

Subsec. (e)(2)(B). Pub. L. 104-294, § 201(4)(A)(iii), added subpar. (B) and struck out former subpar. (B) which read as follows: "which is one of two or more computers used in committing the offense, not all of which are located in the same State;".

Subsec. (e)(8), (9). Pub. L. 104-294, § 201(4)(B)-(D), added pars. (8) and (9).

Subsec. (g). Pub. L. 104-294, § 604(b)(36)(C), substituted "violation of this section" for "violation of the section".

Pub. L. 104-294, § 201(5), struck out ", other than a violation of subsection (a)(5)(B)," before "may maintain a civil action" and substituted "involving damage as defined in subsection (e)(8)(A)" for "of any subsection other than subsection (a)(5)(A)(ii)(II)(bb) or (a)(5)(B)(ii)(II)(bb)".

Subsec. (h). Pub. L. 104-294, § 604(b)(36)(D), substituted "subsection (a)(5)" for "section 1030 (a)(5) of title 18, United States Code" before period at end.

1994-Subsec. (a)(3). Pub. L. 103-322, § 290001(f), inserted "adversely" before "affects the use of the Government's".

Subsec. (a)(5). Pub. L. 103-322, § 290001(b), amended par. (5) generally. Prior to amendment, par. (5) read as follows: "intentionally accesses a Federal interest computer without authorization, and by means of one or more instances of such conduct alters, damages, or destroys information in any such Federal interest computer, or prevents authorized use of any such computer or information, and thereby-

(A) causes loss to one or more others of a value aggregating $1,000 or more during any one year period; or

(B) modifies or impairs, or potentially modifies or impairs, the medical examination, medical diagnosis, medical treatment, or medical care of one or more individuals; or".

ubsec. (c)(3)(A). Pub. L. 103-322, § 290001(c)(2), inserted "(A)" after "(a)(5)".

ubsec. (c)(4). Pub. L. 103-322, § 290001(c)(1), (3), (4), added par. (4).

ubsec. (g). Pub. L. 103-322, § 290001(d), added subsec. (g).

ubsec. (h). Pub. L. 103-322, § 290001(e), added subsec. (h).

990-Subsec. (a)(1). Pub. L. 101-647, § 3533, substituted "paragraph y" for "paragraph r".

ubsec. (e)(3). Pub. L. 101-647, § 1205(e), inserted "commonwealth," before "possession or territory of the United States".

ubsec. (e)(4)(G). Pub. L. 101-647, § 2597(j)(2), which directed substitution of a semicolon for a period at end of subpar. (G), could not be executed because it ended ith a semicolon.

ubsec. (e)(4)(H), (I). Pub. L. 101-647, § 2597(j), added subpars. (H) and (I).

1989-Subsec. (e)(4)(A). Pub. L. 101-73, § 962(a)(5)(A), substituted "an institution," for "a bank".

Subsec. (e)(4)(C) to (H). Pub. L. 101-73, § 962(a)(5)(B), (C), redesignated subpars. (D) to (H) as (C) to (G), respectively, and struck out former subpar. (C) which read as follows: "an institution with accounts insured by the Federal Savings and Loan Insurance Corporation;".

1988-Subsec. (a)(2). Pub. L. 100-690 inserted a comma after "financial institution" and struck out the comma that followed a comma after "title 15".

1986-Subsec. (a). Pub. L. 99-474, § 2(b)(2), struck out last sentence which read as follows: "It is not an offense under paragraph (2) or (3) of this subsection in the case of a person having accessed a computer with authorization and using the opportunity such access provides for purposes to which such access does not extend, if the using of such opportunity consists only of the use of the computer."

Subsec. (a)(1). Pub. L. 99-474, § 2(c), substituted "or exceeds authorized access" for ", or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend".

Subsec. (a)(2). Pub. L. 99-474, § 2(a), (c), substituted "intentionally" for "knowingly", substituted "or exceeds authorized access" for ", or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend", struck out "as such terms are defined in the Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 et seq.)," after "financial institution,", inserted "or of a card issuer as defined in section 1602 (n) of title 15," and struck out "or" appearing at end.

Subsec. (a)(3). Pub. L. 99-474, § 2(b)(1), amended par. (3) generally. Prior to amendment, par. (3) read as follows: "knowingly accesses a computer without authorization, or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend, and by means of such conduct knowingly uses, modifies, destroys, or discloses information in, or prevents authorized use of, such computer, if such computer is operated for or on behalf of the Government of the United States and such conduct affects such operation;".

Subsec. (a)(4) to (6). Pub. L. 99-474, § 2(d), added pars. (4) to (6).

Subsec. (b). Pub. L. 99-474, § 2(e), struck out par. (1) designation and par. (2) which provided a penalty for persons conspiring to commit an offense under subsec. (a).

Subsec. (c). Pub. L. 99-474, § 2(f)(9), substituted "(b)" for "(b)(1)" in introductory text.

Subsec. (c)(1)(A). Pub. L. 99-474, § 2(f)(1), substituted "under this title" for "of not more than the greater of $10,000 or twice the value obtained by the offense".

Subsec. (c)(1)(B). Pub. L. 99-474, § 2(f)(2), substituted "under this title" for "of not more than the greater of $100,000 or twice the value obtained by the offense".

Subsec. (c)(2)(A). Pub. L. 99-474, § 2(f)(3), (4), substituted "under this title" for "of not more than the greater of $5,000 or twice the value obtained or loss created by the offense" and inserted reference to subsec. (a)(6).

Subsec. (c)(2)(B). Pub. L. 99-474, § 2(f)(3), (5)-(7), substituted "under this title" for "of not more than the greater of $10,000 or twice the value obtained or loss created by the offense", "not more than" for "not than", inserted reference to subsec. (a)(6), and substituted "; and" for the period at end of subpar. (B).

ubsec. (c)(3). Pub. L. 99-474, § 2(f)(8), added par. (3).

ubsec. (e). Pub. L. 99-474, § 2(g), substituted a dash for the comma after "As used in this section", realigned remaining portion of subsection, inserted "(1)" before 'the term", substituted a semicolon for the period at the end, and added pars. (2) to (7).

ubsec. (f). Pub. L. 99-474, § 2(h), added subsec. (f).

ffective Date of 2002 Amendment

mendment by Pub. L. 107-296 effective 60 days after Nov. 25, 2002, see section 4 of Pub. L. 107-296, set out as an Effective Date note under section 101 of Title 6, omestic Security.

ransfer of Functions

or transfer of the functions, personnel, assets, and obligations of the United States Secret Service, including the functions of the Secretary of the Treasury relating ereto, to the Secretary of Homeland Security, and for treatment of related references, see sections 381, 551 (d), 552 (d), and 557 of Title 6, Domestic Security, and the epartment of Homeland Security Reorganization Plan of November 25, 2002, as modified, set out as a note under section 542 of Title 6.

eports to Congress

ction 2103 of Pub. L. 98-473 directed Attorney General to report to Congress annually, during first three years following Oct. 12, 1984, concerning prosecutions under is section.

ction Referred to in Other Sections

is section is referred to in sections 981, 982, 1956, 2256, 2332b, 2510, 2516, 3125, 3239 of this title; title 6 section 145; title 8 section 1721; title 17 section 1201; le 26 section 7431; title 31 section 9703.

jolt
UCLA Journal of Law and Technology

Home Career Forum Submissions About Us Articles Archives Notes Note Archives Practice Guide Web Resources

2003 UCLA J.L. & Tech. Notes 6

Federal and California Criminal Violations for Distributed Denial-of-Service Transmissions

by Jacob J. Carroll

Increasingly, a blunt weapon, known as a distributed denial-of-service (DDOS) attack, has been utilized in attempts to flood targeted Internet root servers in order to shut down service. With the increased frequency of these attacks, this Note outlines the mechanisms exercised in such attacks and focuses on federal and California criminal violations for DDOS attacks.

Most recently, an Internet attack targeted the domain name manager UltraDNS with a host of data, causing major delays and difficulties for servers running the host .info and other domains.[1] UltraDNS, a member of the Internet Society, serves as the primary domain name server (DNS) provider for the .org and .info domain names. Ben Petro, CEO of UltraDNS, stated that the assault sent approximately two million requests per second to each device. "This is the largest attack that we've seen," Petro said.[2]

The attack came one month after an identical attack was aimed at similar DNS root servers that many security experts considered the largest and most sophisticated attack ever. The attack used a distributed approach in attacking all of the world's thirteen root servers.[3] The root servers, ten of which are located in the United States, serve as a master directory for the Internet. The DNS system, which converts complex Internet protocol addressing codes into the words and names that form email and Web addresses, relies on the thirteen root servers to tell computers around the world how to reach key Internet domains.[4] At the top of the root server hierarchy is the "A" root server that generates a critical file every twelve hours telling the other twelve servers what Internet domains exist and where they can be found.[5] The DNS is built so that eight or more of the world's thirteen root servers must fail before ordinary Internet users experience degradation. In the recent attack on the .info domain, only four to five of the root servers went down in face of the attack.[6] As a result, end-users did not feel any slowdown.

I. DDOS Attacks

The primary goal of a DDOS attack is to deny a victim's computer, server, or network access to a particular resource.[7] These attacks are characterized by an explicit attempt by a user to deny another user or system from using that service. DDOS attacks can essentially disable individual computers or entire networks. Usually, DDOS attacks can be executed with limited resources against a large and sophisticated site.

Generally, DDOS attacks come in three different forms.[8] The first type of DDOS attack is the consumption of limited or non-renewable resources.[9] This type of attack can vary in its application. Frequently, DDOS attacks are directed at network connections with the goal of preventing the host from communicating to outside networks, or sometimes its own internal network. With this method the attacker begins a process of connecting to the victim's machine, but ultimately never completes the transmission.10 The result is the victim's machine waits to send all other requests until the attacker's request is resolved, which never occurs.11

An alternative method of conducting a DDOS attack occurs when an attacker uses a victim's resources against themselves.12 This is accomplished by forging data packets to connect to the echo service of one machine.13 Ultimately, the echo increasingly repeats through the network, eventually degrading the network substantially.14 A variation of this type of DDOS attack is generating a large number of packets and directing them at a victim's network. In order to increase the frequency and duration of the assault, many attackers will uses dozens, sometimes hundreds, of computers. The end result is completely terminating incoming and outgoing traffic, halting the victim's network activity. Finally, a DDOS attack can be conducted by destroying or altering computer configuration information.15 Improperly configured computers can be modified to perform below optimal speed or can be entirely disabled.

II. DDOS Criminal Legislation

The first version of federal Computer Fraud and Abuse Act (CFAA) was passed in 1984.16 Its purpose was to protect classified, financial, and credit information that was maintained on federal government computers. With the evolution of computing, the CFAA was amended in 1996. This included the removal of "federal interested computers" with the replacement of "protected computer." In this step, Congress effectively broadened the scope of the CFAA from protected federal computers, to exercising federal power over all computers involved in interstate and foreign commerce.17

A. Federal Legislation

The CFAA offers varying degrees of criminal liability for the transmission of DDOS to individuals or corporations.18 Federal criminal violations for DDOS are addressed in Title 18 U.S.C. 1030(5)(A). And, while the standard of knowledge differs between Title 18 U.S.C. 1030(5)(A) and (B), both require the transmission of data or the use of a computer through interstate commerce. The first of these, Title 18 U.S.C. 1030(5)(A) states:

> "through means of a computer used in interstate commerce or communications, knowingly causes the transmission of a program, information, code, or command to a computer or computer system if:
> (I) the person causing the transmission intends that such transmission will -
> (I) damage, or cause damage to, a computer, computer system, network, information, data, or program; or
> (II) withhold or deny, or cause the withholding or denial, of the use of a computer, computer services, systems or network, information, data or program [emphasis added]"

In section A(I), the standard set forth by statue is intentional transmission of data that causes damage or the withholding of the use of a computer or network. The first subsection of Title 18 U.S.C. 1030(5)(A)(I) focuses on damage caused by the transmission of a data set to a computer or computer system. In contrast, the second section of Title 18 U.S.C. 1030(5)(A)(I) aims to criminalize the withholding of the use a computer or a computer system by means of a DDOS or similar attack.

Title 18 U.S.C. § 1030(5)(B) was essentially crafted to mimic Section A of Title 18 U.S.C. § 1030(5). However, Section B requires a lower standard of knowledge to invoke a violation. It states:

> "through means of a computer used in interstate commerce or communication, knowingly causes the

> transmission of a program, information, code, or command to a computer or computer system -
>
> (I) with reckless disregard of a substantial and unjustifiable risk that the transmission will -
>
> (I) damage, or cause damage to, a computer, computer system, network, information, data or program; or
>
> (II) withhold or deny or cause the withholding or denial of the use of a computer, computer services, system, network, information, data, or program [emphasis added]"

The knowledge standard for section B violations is *reckless disregard* (in contrast to section A's *intentional* standard). Essentially, an unintentional denial of a computer or a computer network, without the authorization of the owner can constitute a violation of the statue if the sender acted with reckless disregard to the consequences of his or her actions.

A. California Legislation

The California Penal Code, generally modeled after the federal CFAA, has varying degrees of criminal liability for DDOS.[19] Title 13, Chapter 5, Section 502(a)(5) states that anyone that:

> "knowingly and without permission disrupts or causes the disruption of computer services or denies or causes the denial of computer services to an authorized user of a computer, computer system, or computer network."

Again, while subsection (a) addresses DDOS and similar attacks, Section 8 emphasizes criminalization of data contaminants. Although modeled after the CFAA, the California Penal Code differs in significant ways. Differing markedly on the standard of knowledge required for a violation of the CFAA, the California Penal Code also has no provision for lack of consent by the owner and no minimum dollar amount for a violation to occur. Moreover, the California Penal Code's *knowingly* standard foregoes the *intentional* and *reckless disregard* standard applied by the CFAA, creating a lower knowledge standard for violators. This results in a stricter state penal code for Internet crime than federal law.

III. Conclusion

In conclusion, both federal and California state laws have made efforts to criminalize DDOS attacks. Furthermore, the federal government and the state of California have passed legislation covering a wide range of Internet crime from IP spoofing to virus transmissions. However, as of yet, the effectiveness of most of these laws is relatively unknown. Increasingly, DDOS attacks have become more targeted, sophisticated, and difficult to trace. As such, accelerating DDOS attacks may outstrip current legislation making it difficult or impossible to enforce. So far, it has been the engineers, not the lawyers that have save the Internet root server system and critical network infrastructure security from being jeopardized by DDOS attacks.

inks

Robert Lemos, *Attack Targets .info Domain System*, November 25, 2002, CNET News.com. http://news.com.com/2100-1001-71178.html?tag=mainstry.
Id.
David McGuire, *Attack on Internet Called Largest Ever*, October 22, 2002, Washington Post, tp://www.washingtonpost.com/ac2/wp-dyn/A828-2002Oct22?language=printer.
Id.

[5] *Id.*

[6] *Id.*

[7] *How a Denial-of-Service Attack Works*, February 9, 2000, CNET News.com Staff, http://news.com.com/2100-1017-236728.html?tag=bplst.

[8] Denial of Service Attacks, CERT Coordination Center, June 4, 2001, www.cert.org/tech_tips/denial_of_service.html.

[9] *Id.*

[10] *Id.*

[11] *Id.*

[12] *Id.*

[13] *Id.*

[14] *Id.*

[15] *Id.*

[16] Edmund B. Burke, *The Expanding Importance of the Computer Fraud and Abuse Act*, January 2001, Gigalaw.com, www.gigalaw.com/articles/2001-all/burke-2001-01-all.html.

[17] Edmund B. Burke, Computer Usage Policies and the Computer Fraud and Abuse Act, February 2001, Gigalaw.com, www.gigalaw.com/articles/2001-all/burke-2001-02-all.html.

[18] To view Title 18 U.S.C. 1030 in its entirety go to http://www.usdoj.gov/criminal/cybercrime/1030_new.html. Please note that this paper only discusses selected section of Title 18 U.S.C 1030. Title 18 U.S.C 1030 breadth is very broad and includes coverage for federal computers, financial institutions, U.S. department and agencies, as well as, prosecution on physical injuries sustained and threats to public health.

[19] To view Title 13, Chapter 5, Section 502(A) in its entirety go to http://www.leginfo.ca.gov/cgi-bin/displaycode?section=pen&group=00001-01000&file=484-502.9.