UNITED STATES DISTRICT COURT
District of New Jersey

Harold C. "Hal" Turner D/B/A Turner Radio Network D/B/A Hal Turner Radio Show Plaintiff,	:	Hon. Civil Action No. 07CV306 (PGS)
V.	:	
4Chan.org 7chan.org Ebaumsworld.com NexisOnline.net Abjects.com John Doe(s) 1-1000 Defendants:	:	COMPLAINT

Plaintiff, Harold C. "Hal" Turner by way of Complaint against the internet web sites 4chan.org, 7chan.org, ebaumsworld.com, nexisonline.com and abjects.com and John Doe(s) 1-1000 hereby says:

I. THE PARTIES

1. Plaintiff Harold C. "Hal" Turner is and at all relevant times was a citizen of the State of New Jersey and the United States of America, residing at 1906 Paterson Plank Road, North Bergen, Hudson County, New Jersey within this District, doing business as Turner Radio Network and The Hal Turner Radio Show.

2. Upon information and belief Defendant 4chan.org is an internet web site whose owner information is presently intentionally concealed and unavailable absent a Subpoena, but whose business and activities relevant to this Complaint took place substantially within this District.

3. Upon Information and belief, Defendant 7chan.org is an internet web site whose owner information is presently intentionally concealed and unavailable absent a Subpoena, but whose business and activities relevant to this Complaint took place substantially within this District.

4. Upon information and belief, Defendant Ebaumsworld.com is an internet web site whose owner information shows an address of eBaums World PO BOX 18091 Rochester, New York 14618 , but whose business and activities relevant to this Complaint took place substantially within this District

5. Upon information and belief, Defendant Nexisonline.net is an internet web site whose owner information indicates

it is a California corporation, Nexis Entertainment located at 1675 Garnet Lane Concord, CA 94519 but whose business and activities relevant to this Complaint took place substantially in this District

6. Upon information and belief, Defendant Abjects.com is an internet web site whose owner information shows it is a corporation Velocity Enterprises 1006 E. Market St, York, PA 17320 whose business and activities relevant to this Complaint took place substantially within this District.

7. Upon information and belief, Defendants John Doe 1-1000 are presently unknown individuals acting in concert with the named Defendants above, and whose activities relevant to this Complaint took place substantially within this District.

II. JURISDICTION AND VENUE

8. This Court has original jurisdiction over Plaintiff's claims pursuant to 28 U.S.C. 1338 (a) (original jurisdiction in cases involving infringement of Copyright), 28 U.S.C. 1331 (federal question) and 28 U.S.C. 1367(a) (supplemental jurisdiction)

9. The matter in controversy exceeds the sum of $50,000 exclusive of interest and costs

10. Venue is proper in this judicial District pursuant to 28 U.S.C. 1391(b)(2) because a substantial part of the actions giving rise to Plaintiff's claim have occurred in this District.

III. FACTUAL BACKGROUND

A. The Business of the Plaintiff

11. Plaintiff owns a Computer Server which is co-located in a Data Center in Parsippany, NJ. Through this computer server, Plaintiff engages in Interstate Commerce by operating several internet web sites, HalTurnerShow.com, TurnerRadioNetwork.com, PrivateWebHosting.org. Through these sites, Plaintiff provides web site hosting services for individuals and groups needing such services and provides interstate communication services for the broadcast of cyber-radio shows by Plaintiff and other individuals and groups. One such cyber-radio show is "The Hal Turner Show." While it is being broadcast live on the Internet "The Hal Turner Radio Show" (hereafter referred to as "The Show") is the single, most-listened-to talk radio program in the entire world on the America Online (AOL)/SHOUTcast internet streaming audio system. While it airs, The Show has more

listeners on the internet than radio station WNYC AM 820, in New York City; more listeners on the Internet than radio station WBUR 90.9 FM in Boston, MA; and is growing in popularity and listenership. The reasons The Show is so popular has to do with unfettered free speech afforded to callers and exercised by Plaintiff as Host. People can call-in and use any language or terminology they choose, to express their thoughts or feelings about social, political, cultural, racial or religious issues, without fear of being censored or cut off. The Show is the literal embodiment of the First Amendment to the Constitution for The United States of America. The Show is a national treasure.

12. Allowing and exercising such unfettered free speech has caught the attention of a number of self-anointed arbiters of political correctness who seem to think they have a right to decide for others, what should and should not be allowable public discourse. These self anointed, politically correct tyrants have, for the six years that the Show has aired, used every method possible to stifle, censor, smear, vilify, besmirch, disrupt, interrupt and shut down The Show. All their efforts have failed, until now.

B: Actions Leading To This Complaint

13. At some point prior to December 20, 2006, a group of self-anointed tyrants utilized an internet relay chat (IRC) known as irc.abjects.com in a chat room called #halturner, to concoct and implement a scheme to disrupt The Show by placing dozens of crank calls while the show aired. Since callers to The Show are not pre-screened for content, they were able to get on the air and pull their pranks, thus successfully disrupting the program for the three hours it aired.

14. After The Show ended, Plaintiff decided to research the Caller ID for phone lines coming into The Show. The research allowed plaintiff to identify five or six specific telephone numbers that had repeatedly called The Show. Two days later, on December 22, 2006, Plaintiff chose to publicly release those phone numbers via the web site HalTurnerShow.com as a warning to others not to engage in that type of activity anymore.

15. When Plaintiff released those phone numbers, the John Doe Defendants named in this action at law - and hundreds of their John Doe cohorts from the Defendant's web sites - became enraged that Plaintiff dared to fight back.

16. Later, on or about December 23, 2007, one or more of the John Does posted to the internet Plaintiff's personal, private, unlisted home telephone number and the private unlisted home telephone number of Plaintiff's 62 year old mother, Kathleen Diamond in Tunkhannock, PA.

17. Within hours of the publishing of the private unlisted home telephone numbers above, Plaintiff began to receive dozens of harassing, abusive and threatening calls. The first such call was received by Plaintiff's wife, Phyllis Turner. Plaintiff later came to find that the John Doe Defendant caller recorded that call and publicly published the audio on the Internet for others to hear in direct violation of 47 U.S.C. 605(a). This had the effect of encouraging hundreds of others to engage in the same activity. These calls continued into all hours of the day and night, continued throughout Christmas Eve and Christmas Day and became so bothersome that Plaintiff had to shut off his telephone and, ultimately, change his telephone number.

18. Almost simultaneously with the calls to Plaintiff's home, Plaintiff's 62 year old mother who lives with her 70 year old husband in Tunkhannock, PA, started receiving

similar calls. So determined were these John Doe Defendants to disrupt and harass, they continued to place these harassing and threatening calls throughout Christmas Eve and even on Christmas Day. These calls became so bothersome to Plaintiff's mother and her husband - who is recovering from Leukemia - they too had to change their telephone number.

19. At or about 12:30 PM EST on December 23, 2006, Plaintiff examined the real-time, graphical data-flow chart for his computer server. That real-time graphical data-flow chart showed the computer server had begun to receive extraordinary amounts of internet data traffic. Data flow out of the computer server suddenly increased about 100 times the normal rate. This became very worrisome very quickly because Plaintiff must pay for all data that flows into and out of the computer server. Plaintiff logged-in to the administrative area of the computer server and called up a "Netstat" report to identify what connections were being made to the computer server. Plaintiff found thousands of simultaneous connections from dozens of users, but these connections were strange: They were emanating from the same Internet Presence (IP) addresses. These connections to Plaintiff's computer server were systematically and

deliberately calling for, and receiving, tens of thousands of exact duplicate copies of Plaintiff's web sites and / or exact duplicates of certain files on those sites. These exact duplicates were all going to the exact same computers on the exact same day(s).

20. In common internet parlance, data flow into and out of a computer server is known as "bandwidth" and the type of activity described in #18 above, being done to Plaintiff's computer server, is commonly called "Bandwidth rape." It is a malicious form of data leeching activity designed specifically to suck the data out of a web site, so thoroughly and for so long, that the site is financially killed by increased bandwidth costs.

21. Upon realizing what was happening, Plaintiff began to analyze the logs of connections to the computer server using the "Netstat" command which shows all connections. Those logs helped to isolate and allow the blocking of the offending IP addresses. Plaintiff contacted the data center where the server is located and asked them to begin blocking the worst offending IP addresses. They did. The server bandwidth started returning to normal.

22. Apparently, the attackers realized they were being blocked out, so they publicly published messages on the one or more of the Defendants web sites, asking others to join in the attacks and providing detailed instructions about how to perpetrate the attacks. The data flow once again jumped to 100 times normal. Late in the day on December 23, or early in the morning on December 24, Plaintiff decided to temporarily shut off the web sites hoping that the attackers would go away.

23. Over the Christmas holiday, Plaintiff researched Bandwidth rape and learned that it can be defended against by installing a file which tells automated software that Plaintiff's sites will not accept their use. Plaintiff installed on the computer server a file called "robots.txt" which instructs automated software that my computer server will not accept their connections. Plaintiff thought the problem was solved. It was not.

24. On December 26, 2006 Plaintiff turned the web sites back on and almost immediately attacks began anew, but in a different, more destructive form: SYN-ACK data packet floods.

25. When one computer tries to communicate with another computer over the Internet, the origin computer sends a "SYNCHRONIZE (SYN)" data packet to the target computer it is trying to reach. This data packet tells the target computer to prepare to communicate with the origin computer via certain internet addresses, IP's. The target computer then sets aside a small amount of its resources to be able to handle whatever the origin computer needs and sends and ACKNOWLEDGEMENT (ACK) data packet to the origin computer saying it is ready to communicate. In a SYN-ACK flood attack, the origin computers deliberately send a SYN data packet but never follow through with communication. This is a malicious act because as the target computer sets aside resources to prepare to communicate with tens of thousands of these origin SYN requests, the resources of the target computer get used up, making the computer unable to continue handling other, legitimate SYN requests. This type of activity is specifically designed to cause the target computer to be unavailable to legitimate users, who, when they try to connect, can get no reply from the targeted computer because its resources have become overloaded.

26. Since SYN-ACK data packets are absolutely essential to the proper operation of computer communication via the

internet, there is absolutely no technological defense that Plaintiff is aware of, which can prevent this type of attack. As such this type of activity - designed to make data unavailable - was specifically outlawed by the Computer Fraud and Abuse Act 18 USC 1030.

27. For the purposes of this Complaint, Plaintiff's computer server is a "protected computer" as defined in 18 USC 1030 because it is "used in interstate commerce" for the purpose of "communication." Hence, the provisions of 18 USC 1030 apply to Plaintiff's computer server.

28. On December 28, 29 and 31, 2006, additional SYN-ACK attacks were launched against Plaintiff's computer, flooding it with upwards of 100 times the normal inbound data, which Plaintiff has to pay for, and making it impossible for the computer server to handle legitimate communication requests. On December 31, 2006, Plaintiff had to shut off his web sites again to protect from being Bankrupted by these attacks.

29. On or about Tuesday, December 26, Plaintiff received an e-mail from a local Papa Johns Pizza Store advising they were filling my internet order for about $93 in pizza and stating the pizzas would be delivered soon. Plaintiff placed no such order. Plaintiff called the

store to cancel it and told them it was a case of WIRE FRAUD.

30. On or about Wednesday, December 27, Plaintiff once again aired "The Hal Turner Show" which ended around 11:00 PM EST. At about 1:00 AM on Thursday, December 28, our home doorbell rang waking up Plaintiff and his family. It was a Pizza delivery from a local pizza store, filling another Pizza order which Plaintiff did not place. The pizza delivery man showed me his delivery slip which showed Plaintiff's name, address and telephone number. Plaintiff placed no such order. Plaintiff told the delivery person this was another case of WIRE FRAUD.

31. On or about Friday, December 29, at about 1:00 in the afternoon, Plaintiff's home doorbell rang again with yet another pizza delivery, this one telephoned into the pizza shop by someone fraudulently claiming to be Plaintiff, but which Plaintiff did not order. As before, the pizza delivery man showed Plaintiff a delivery slip with Plaintiff's name, address and home telephone number. Plaintiff placed no such order and told the delivery person this was another case of WIRE FRAUD.

32. On or about Saturday, December 30, 2006, two large boxes were delivered to Plaintiff's home by the United States Postal Service. Inside were bulk amounts of shipping boxes shipped to Plaintiff's home by the internet auction web site, EBAY.com. These boxes are shipping supplies which are designed to allow EBAY sellers to ship goods to EBAY buyers. Plaintiff placed no such order for any such supplies. Plaintiff has told EBAY this was a case of MAIL FRAUD and EBAY told Plaintiff to ship the supplies back to them.

33. Since these attacks commenced, Plaintiff has received e-mails and electronic messages posted to his web site visitor comments area trying to Extort a surrender. The wording varied, but the message is the same: "We will not stop until you shut down your web site and your radio show." This attempt to force Plaintiff to do something he is unwilling to do - terminate a lawful $60,000 per year and growing enterprise - is Extortion.

34. On January 3, 2007, during Plaintiff's live radio show which airs from 9:00 PM until 11:00 PM EST, the computer server suffered the largest, most disruptive attack to date. A sudden and dramatic increase of inbound traffic

hit the server at six-hundred-sixty megabits per seconds (660 Mbps.) This attack was so enormous and so sustained that it saturated routers in the data center, taking Plaintiff's web sites off line and also halting normal computer data flow for hundreds of other customers whose computers are also inside the data center. So damaging was this attack that the data center had to "null route" (shut off all access to) the computer server, rendering Plaintiff unable to conduct a radio show or to do business through that server for the next ten hours, until the data center could clear the inbound data backlog.

35. On or about Friday, January 5, 2007, a Manager from the United States Post Office at North Bergen, NJ came to Plaintiff's home to ask if he had ordered a truckload of postal shipping supplies. Plaintiff told him no. The Postal manager advised that the North Bergen Post office had one or more Pallets of shipping supplies, allegedly ordered by Plaintiff, but they were hesitant to deliver it because it appeared to be a fraud. Plaintiff told the Postal Manager it was, in fact additional mail fraud and the manager told Plaintiff he would alert U.S. Postal Inspectors for federal investigation.

36. On or about Friday, January 5, 2007, the owners of web site 7chan.org removed the front page of their site and put in its place an apology to Plaintiff. The page showed an image of a Five Dollar Bill, with an altered photograph of Plaintiff in the middle of that bill, and the caption above the bill read as follows" WE'RE SORRY WE TOOK ALL UR MONIES, HERE" as if to give Plaintiff the fake five dollar bill. This act appears to be an overt acknowledgement that Defendant 7chan.org deliberately attacked my web site and deliberately cost me money.

37. On or about January 4, 2007 I received an email from a person calling himself Joey Bernert, purporting to be an administrator, a person in authority at the web site ebaumsworld.com. That e-mail acknowledged that their site supported the attacks launched against Plaintiff, which indicates they were willing participants, facilitators or accessories to the acts described herein.

38. On January 3, another Denial of Service attack was launched at Plaintiff's server, taking The Show off the internet.

39. On January 9, 2007, Plaintiff was notified in writing by Net Access Corporation, that due to the repeated

Denial of Service attacks against the server, they will not continue service to Plaintiff. They further advised that if future inbound attacks occurred, they would be forced to immediately halt service to me so as to protect their other customers. Their letter requires Plaintiff remove the server from their data center on or before February 15. While Plaintiff has made arrangements for a new data center to provide service, the cost for such service is sixty-one percent (61%) more expensive per month at minimum. If these Denial of Service attacks continue, the added costs and possibility of being thrown out of the new data center are causing incalculable harm to Plaintiff.

40. On January 10 and 17, two additional Denial of Service attacks occurred against Plaintiff's server, both organized and promoted on the Defendant(s) web sites. The attack on the 17th, forced Net Access Corporation to once again 'null route" Plaintiff's server to protect their other data center customers.

41. On January 18, 2007, a number of regular visitors to Plaintiff's web site telephoned saying they could not access Plaintiff's sites. Upon investigation, Plaintiff

determined that Net Access Corporation has, in fact, null routed access to the server again to protect their other customers and as a result, Plaintiff is effectively out of business because of the Denial of Service attacks.

C. The Business of the Defendants

42. 4chan.org is an internet web site that allows users to post messages and images of various types seemingly without restraint. Criminal activity seems to be rampant and well documented on this web site. The site contains pornographic depictions of children and well publicized terrorist bombing threats. The Court's attention is directed to an incident which occurred in October 2006. Late that month, the United States Department of Homeland Security issued a nationwide terrorist attack alert over the alleged planned truck bombings of NFL Football Stadiums. The threats to truck-bomb those stadiums was posted on the web site 4chan.org upwards of forty (40) separate times before authorities arrested the perpetrator.

43. 7chan.org is an internet web site that allows users to post messages and images of various types. Criminal activity on this web site includes pornographic

depictions of children and photographs of pre-teen and teenage girls in various states of undress. One area of this site is specifically set up to foster criminal attacks against other web sites. That area, called /i/ for INVASION allows users to anonymously conspire together, in public, to arrange criminal attacks against various web sites around the world similar to the attacks outlined in this Complaint.

44. Ebaumsworld.com is an internet web site offering examples of prank phone calls and telephone harassment against a variety of targets similar to those outlined in this complaint. The site also offers a message forum in which users can talk about various topics or plan and coordinate illegal activities against a variety of web sites similar to those outlined in this complaint.

45. NexisOnline.net is an internet web site which offers IRC chat and the ability to download "malware." Malware is malicious computer software which can be used to attack internet users and web sites similar to the attacks outlined in this complaint.

46. Abjects.com is an internet web site offering free Internet Relay Chat (IRC) through which its users can

talk about a variety of topics including planning illegal attacks against computer servers as outlined in this complaint.

47. The business of John Doe(s) 1-1000 is not known at this time.

COUNT ONE

COPYRIGHT INFRINGEMENT (17 U.S.C. 501 et. seq.)

48. John Doe Defendants perpetrated infringement upon Plaintiff's Copyright by making copies of his radio shows of December 20 and December 27, posting copies of those shows on free file storage services and then advertising a link on the named Defendants web sites encouraging users to take copies of those shows. By making the shows available free, the general public was able to avoid paying Plaintiff for subscription access to such shows, thus causing incalculable harm to plaintiff in lost revenues from subscription sales. By allowing users to post links to the infringed material, named Defendants facilitated wide distribution of the infringed material.

49. Further irreparable harm to Plaintiff is imminent as a result of Defendants conduct and Plaintiff is without an adequate remedy at law. Plaintiff is entitled to

injunctive relief, restraining named defendants, their agents, employees, representatives and all persons acting in concert with them from engaging in further Copyright infringement.

50. Plaintiff is further entitled to recover from Defendants, monetary damages as a result of defendant's acts of Copyright Infringement in an amount to be determined at trial.

51. Plaintiff is also entitled to recover from Defendants, the gains, profits and advantages they have obtained as a result of their acts of copyright infringement in an amount to be determined at trial.

COUNT TWO

COMPUTER FRAUD AND ABUSE 18 U.S.C. 1030)

52. John Doe Defendants willfully engaged in activities specifically designed to cause the data on Plaintiff's server to be made "unavailable." The named Defendants willfully facilitated, aided and abetted those activities by allowing users of their web sites to conspire, plan, organize, incite and teach others how to commit similar acts via their web sites, and in the case of Defendant

7chan.org, by featuring a specific area of their web site designed to aid, abet and further attacks against internet web sites.

COUNT THREE

COMMON LAW FRAUD

53. John Doe Defendants engaged in Common Law Fraud in violation of the laws of the State of New Jersey by intentionally using automated software to repeatedly download content from my web sites for the sole purpose of causing harm in the form of increased bandwidth costs. These acts deprived Plaintiff of the inestimable right of fair dealing and were done with malice for the sole purpose of inflicting financial harm. Named Defendants willfully facilitated, aided and abetted this Fraud by allowing users of their web sites to conspire, plan and organize these acts through publishing instructions on the methods and tasks to be undertaken for the purpose of harming Plaintiff.

COUNT FOUR

MAIL FRAUD

54. John Doe Defendants committed numerous acts of mail fraud by placing orders for goods, services and merchandise to be shipped to Plaintiff via United States

Postal Service, with Plaintiff being billed for such goods and merchandise, when Plaintiff made no such requests for any goods, services or merchandise. Named defendants facilitated, aided and abetted such Mail Fraud by allowing users of their web sites to conspire, plan, organize and incite such acts via their web sites.

COUNT FIVE

WIRE FRAUD

55. John Doe Defendants committed numerous acts of Wire Fraud by placing orders via telephone for goods, services and merchandise to be shipped to Plaintiff, with Plaintiff being billed for such goods and merchandise, when Plaintiff made no such requests for any goods, services or merchandise. Named defendants facilitated, aided and abetted such Wire Fraud by allowing users of their web sites to conspire, plan, organize and incite such acts via their web sites.

COUNT SIX

EXTORTION

55. John Doe Defendants committed extortion by demanding Plaintiff quit, shut down and/or cancel his radio show and web sites under threat of continuing Computer Fraud and Abuse, Mail Fraud, Wire Fraud. Attempting to force

someone to give up his radio show and web sites, an estimated $60,000 per year enterprise which is something of value, under such threats of continued computer attacks and fraud is extortion. Named Defendants facilitated, aided and abetted such Extortion by allowing users of their web sites to publicly and repeatedly conspire, plan, organize and implement the attacks in furtherance of the effort to force Plaintiff to give up his business.

COUNT SEVEN

RACKETEER INFLUENCED CORRUPT ORGANIZATION(S) (18 U.S.C. 1961-1968)

56. Since two or more people from each of the named Defendant web sites, acting in concert, engaged in the "predicate felonies" of Mail Fraud, Wire Fraud and Extortion, within a ten year period, and since the named defendants 4chan.org, 7chan.org, Ebaumsworld.com, Nexisonline.net and Abjects.com, willfully facilitated, aided and abetted these acts, the named defendants are, in fact, Racketeer Influenced, Corrupt Organizations. Pursuant to 18 U.S.C. 1964(a) Plaintiff is entitled to triple damages in an amount to be determined at trial.

Whereas Plaintiff has suffered substantial harm as outlined above and has no other remedy at law, Plaintiff hereby demands a Trial by jury to recover monetary damages as a jury may see fit to award.

I declare under penalty of perjury and pursuant to 28 U.S.C. 1746 that the foregoing is true and correct.

Dated: North Bergen, New Jersey

January 19, 2007

BY:

Harold C. "Hal" Turner

Plaintiff