

JUDGE MARSHA J. PECHMAN

IN THE UNITED STATES DISTRICT COURT  
WESTERN DISTRICT OF WASHINGTON  
AT SEATTLE

UNITED STATES OF AMERICA,	)	
	)	
<i>Plaintiff,</i>	)	NO. CR07-187MJP
	)	
v.	)	<b>DEFENDANT'S SUPPLEMENTAL</b>
	)	<b>SENTENCING MEMORANDUM</b>
ROBERT ALAN SOLOWAY,	)	
	)	
<i>Defendant.</i>	)	
_____	)	

COMES NOW the defendant, ROBERT ALAN SOLOWAY, and submits this Supplemental Sentencing Memorandum to address (1) the testimony of Dr. John Levine and the issue of "opt-in" email, and (2) the Government's Response to Defendant's Sentencing Memorandum.

I. INTRODUCTION.

On Friday, July 11, 2008, Dr. John R. Levine testified as an expert for the government. The subject of his testimony was "spam" on the internet. When asked to define spam, Dr. Levine responded that he defined spam as "unsolicited bulk commercial email." Much of his later testimony incorporated this definition. The CAN-SPAM violation, 18 U.S.C. §1037(a), to which Mr. Soloway pled guilty, does not use the term

COPY

1 "unsolicited." Rather, it uses the terms "multiple commercial electronic mail messages."

2 The subject of "opt-in" email addresses also arose. In fact, the Court asked Dr.  
3 Levine some specific questions regarding "opt-in" email addresses, including asking him  
4 to specifically explain the meaning of that term. Dr. Levine opined that "opt-in" email  
5 address means that it is the email address of a person who has either solicited, or agreed  
6 to accept, email from a particular person or on a particular subject. However, on cross-  
7 examination Dr. Levine had to agree that he didn't know if "opt-in email addresses" is  
8 even mentioned in the CAN-SPAM Act. It is not.  
9

10 Significantly, the entire discussion of "opt-in" email addresses centered on whether  
11 such email could be considered "unsolicited" in order to meet Dr. Levine's definition, not  
12 the definition used in the statute. Indeed, cross-examination developed that others within  
13 the computer world have differing definitions of opt-in. Ultimately, Dr. Levine testified  
14 that he would not want to venture an opinion as to how many times a list of opt-in email  
15 addresses would have to be sold before it ceased to be considered opt-in. Dr. Levine also  
16 had to admit that what is spam and what isn't spam is still very confusing, even to  
17 someone with his extensive internet background and expertise.  
18  
19

## 20 II. ARGUMENT.

### 21 A. THE CAN-SPAM ACT DOES NOT LIMIT THE TRANSMISSION OF COMMERCIAL 22 ELECTRONIC MAIL MESSAGES TO ONLY PEOPLE WHO HAVE AFFIRMATIVELY 23 REQUESTED TO RECEIVE IT.

24 The criminal provisions of the CAN-SPAM Act (18 U.S.C. §1037) do not include  
25 the term "opt-in" email address, nor do they even address the concept of opt-in email  
26 addresses. The civil provisions do, however, address the opposite concept, known as the  
27 opt-out provision.

1 Section 5(a)(3) of the CAN-SPAM Act requires that all commercial electronic mail  
2 messages include a mechanism whereby the recipient can request not to receive future  
3 commercial electronic mail messages from that sender at the email address where the  
4 message was received, and by doing so opt out of the list. Section 5(a)(4) prohibits the  
5 transmission of commercial electronic mail to the email address of a recipient who has  
6 opted out.  
7

8 Thus, the Act requires the recipient to opt-out of receiving future emails from a  
9 particular sender. So long as the other regulatory provisions of the Act are met, nowhere  
10 does the act prohibit someone from sending bulk commercial email to someone who has  
11 not opted in and specifically requested it. The Act only prohibits the transmission to  
12 someone who has expressly objected to receiving it, and even then it results only in a civil  
13 penalty and is not a criminal offense.  
14

15 **B. THE NUMBER OF VICTIMS.**

16 The government argues, at pages 2-3, that the Court can make reasonable  
17 inferences from the evidence, and that based on its "representative recipients" of Mr.  
18 Soloway's email, the Court can conclude that there were more than 250 "victims" in this  
19 case. First, the government's witnesses were hardly "representative" of the typical  
20 recipient of Mr. Soloway's email messages. If they were truly representative, one may  
21 fairly ask why it was necessary to fly them to Seattle, at taxpayer expense, from Florida,  
22 Wisconsin, Pennsylvania, California, Michigan, Oklahoma, Ohio, and England to testify.  
23 Were there not any "representative" victims in the State of Washington? We submit that  
24 these witnesses were far from being representative, and that the typical person who  
25 received Mr. Soloway's email messages simply captured them in a Spam filter, or deleted  
26  
27  
28

1 them with the stroke of a key.

2 Second, the government ignores the guidelines definition of "victim," which  
3 requires a pecuniary loss. U.S.S.G. §2B1.1, Application Note 3(A)(iii).  
4

5 **C. THE TIMING OF THE FILING OF DEFENDANT'S SENTENCING MEMORANDUM.**

6 Defendant received, via email, a copy of the final Presentence Report at around  
7 1:00 p.m. on Monday, July 7. We needed to know what was in the final PSR before we  
8 could file our sentencing memorandum, especially because of the number of written  
9 objections we had previously filed to the draft. Without knowing which, if any, of those  
10 objections had resulted in corrections to the final report, it was simply not possible to  
11 submit a meaningful sentencing memorandum to the Court.  
12

13 **D. THE GOVERNMENT HAS PROVIDED NO EVIDENCE THAT MR. SOLOWAY SENT EMAILS  
14 TO THIRD PARTIES USING ANOTHER PERSON'S EMAIL ADDRESS, OTHER THAN  
THOSE IN WHICH THE "TO" AND THE "FROM" WERE THE SAME.**

15 The government complains that the defense has "misrepresented" the facts by  
16 claiming that the government has not produced any evidence that Mr. Soloway sent email  
17 to third parties using other people's email addresses. In fact, the government has not  
18 produced any such evidence, and the four Middleton emails are discussed in the  
19 Defendant's Sentencing Memorandum, at page 16, lines 9-16. At best, the government  
20 has produced evidence that some people claim that email was sent to third parties using  
21 their email address, but the government has produced no evidence that those emails came  
22 from Mr. Soloway. Nor do the four Middleton emails support the government's  
23 argument.  
24

25 There are a total of four emails (out of the hundreds of millions of email the  
26 government contends Mr. Soloway sent) that the government has provided to the defense  
27

1 that appear to have been sent to "consuelo@consuelogonzalez.com," and which appear to  
2 have come from someone at the domain name of "richardmiddleton.net." These emails  
3 appear to have been sent as part of the broadcast email service that Mr. Soloway provided  
4 to customers of his broadcast email service for a fee. These emails were apparently only  
5 sent to Mr. Middleton's wife (Consuelo Gonzalez), and there is only one such email for  
6 each of four customer ads. Mr. Middleton has not claimed that he is aware of any other  
7 such emails using his domain name, nor did he receive any "bouncesbacks." If a broadcast  
8 email had been done using Mr. Middleton's domain name, he would likely have received  
9 thousands of bouncebacks, and numerous complaints from other internet users, and that  
10 did not happen. Thus, it appears that these emails were sent only to his wife.  
11  
12

13 The domain names "consuelogonzalez.com" and "richardmiddleton.net" were both  
14 registered with the internet provider westserver.net on November 17, 2000, at 8:56 p.m.  
15 and 8:57 p.m., respectively. It thus appears as though there may be some automatic  
16 forwarding program between these two domain sites, because the odds of these four emails  
17 with Mr. Middleton's domain name going only to his wife's domain, and to no one else,  
18 are astronomical.  
19

20 Finally, those four emails did not contain the email address of a real person. While  
21 the domain name was registered to Mr. Middleton, there are no real people, and no real  
22 email addresses, as set forth in the "from" field in those emails.  
23

24 **E. THE JEREMY JAYNES CASE IS NOT COMPARABLE TO THIS CASE.**

25 On Friday, July 11, the defense submitted some supplemental sentencing materials,  
26 which consisted of pleadings from two other computer cases. Rather than attempting to  
27 put its own "spin" on the facts of those cases, the defense included the charging document  
28

1 from each case, together with either the plea agreement (Downey) or the government's  
2 sentencing letter (Smathers), and the respective judgments. We left it to the Court to  
3 decide if comparisons with this case were appropriate.  
4

5 On the other hand, the government is now arguing that a Virginia state case,  
6 brought under a Virginia state statute (not the federal CAN-SPAM Act) involving Jeremy  
7 Jaynes, is an apt comparison to this case. However, the government chose to provide only  
8 the facts of that case that it wanted the Court to know about. Specifically, the government  
9 describes that case as follows:  
10

11 Jaynes sent over 10,000 "pieces of unsolicited bulk e-mail"  
12 (spam) with forged headers, and relayed through proxies, on  
13 each of three different days in July of 2003, from his home  
14 in North Carolina to more than 50,000 AOL e-mail  
subscribers. (The total volume of the spam on these three  
days was approximately 60,000).

15 The government left out a few details that this Court might want to be aware of in  
16 comparing that case to Mr. Soloway's case. These facts, taken from the Virginia Supreme  
17 Court opinion upholding his conviction, 4-3, include the following:

18 1. While executing a search of Jaynes' home, police discovered a  
19 cache of compact discs (CDs) containing over 176 million full e-mail  
20 addresses and 1.3 billion email user names;

21 2. The search also led to the confiscation of a storage disc which  
22 contained AOL e-mail address information and other personal and private  
account information for millions of AOL subscribers;

23 3. Police also discovered multiple storage discs which contained  
24 107 million AOL e-mail addresses;

25 4. Richard Rubenstein, manager of technical security investigations  
26 at AOL, testified that the discs recovered in Jaynes' home "contained  
27 proprietary information" of "pretty near all" AOL account customers. The  
AOL user information had been stolen from AOL by a former employee  
and was in Jaynes' possession;  
28

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

5. Jaynes' emails marketed a number of fraudulent products;

6. Jaynes' income from his fraudulent business exceeded \$1,000,000.00 in each of the years 2001, 2002, and 2003;


7. Jaynes had amassed assets worth \$17,000,000.00 and a net worth of \$24,000,000.00;

8. Jaynes was released on a \$1,000,000.00 bond pending appeal.

Additional facts are set forth in a number of news articles about the case, which include the fact that Jaynes was allegedly making between \$400,000.00 and \$700,000.00 each and every month from his fraud scheme. A copy of the Virginia Supreme Court opinion containing the "Background and Material Proceedings Below" is attached hereto as Exhibit A. The Court may draw its own conclusions as to the government's attempt to portray the Jaynes case as merely involving the sending of 60,000 emails with forged headers and using proxies over a three day period.

DATED this M day of July, 2008.

RICHARD J. TROBERMAN, P.S.

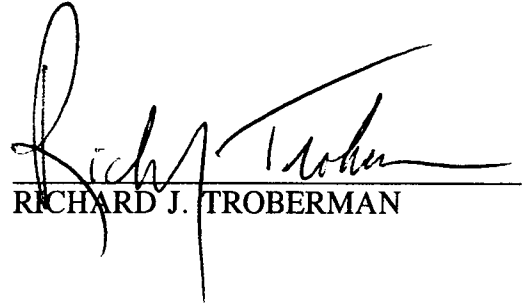
By: 

RICHARD J. TROBERMAN  
WSBA #6379  
Attorney for Defendant  
Robert Alan Soloway

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

CERTIFICATE OF SERVICE

I hereby certify that on July ~~7~~<sup>15</sup>, 2008, I electronically filed the foregoing "Defendant's Supplemental Sentencing Memorandum" with the Clerk of Court, using the CM/ECF system which will send notification of such filing to the attorneys of record in this case.

  
RICHARD J. TROBERMAN

# **EXHIBIT A**

Present: Hassell, C.J., Koontz, Kinser, Lemons, and Agee, JJ.,  
and Russell and Lacy, S.JJ.

JEREMY JAYNES

v. Record No. 062388

COMMONWEALTH OF VIRGINIA

OPINION BY  
JUSTICE G. STEVEN AGEE  
February 29, 2008

FROM THE COURT OF APPEALS OF VIRGINIA

Jeremy Jaynes appeals from the judgment of the Court of Appeals which affirmed his convictions in the Circuit Court of Loudoun County for violations of Code § 18.2-152.3:1, the unsolicited bulk electronic mail (e-mail) provision of the Virginia Computer Crimes Act, Code §§ 18.2-152.1 through - 152.15. For the reasons set forth below, we will affirm the judgment of the Court of Appeals.

I. BACKGROUND AND MATERIAL PROCEEDINGS BELOW

From his home in Raleigh, North Carolina, Jaynes used several computers, routers and servers to send over 10,000 e-mails within a 24-hour period to subscribers of America Online, Inc. (AOL) on each of three separate occasions. On July 16, 2003, Jaynes sent 12,197 pieces of unsolicited e-mail with falsified routing and transmission information onto AOL's proprietary network. On July 19, 2003, he sent 24,172, and on July 26, 2003, he sent 19,104. None of the recipients of the e-mails had requested any communication from Jaynes. He intentionally falsified the header information and sender domain

names before transmitting the e-mails to the recipients, causing the Internet Protocol (IP) addresses to convey false information to every recipient about Jaynes' identity as the sender.<sup>1</sup>

However, investigators used a sophisticated database search to identify Jaynes as the sender of the e-mails.<sup>2</sup> Jaynes was arrested and charged with violating Code § 18.2-152.3:1, which provides in relevant part:

- A. Any person who:
  - 1. Uses a computer or computer network with the intent to falsify or forge electronic mail transmission information or other routing information in any manner in connection with the transmission of unsolicited bulk electronic mail through or into the computer network of an electronic mail service provider or its subscribers . . . is guilty of a Class 1 misdemeanor.
  
- B. A person is guilty of a Class 6 felony if he commits a violation of subsection A and:
  - 1. The volume of UBE transmitted exceeded 10,000 attempted recipients in any 24-hour period, 100,000 attempted recipients in any 30-day time period, or one million attempted recipients in any one-year time period. . . .

---

<sup>1</sup> Simple Mail Transfer Protocol (SMTP) is what an e-mail server uses to transmit an e-mail message, and the SMTP requires verification of the sender's IP address and domain. Evidence at trial demonstrated that Jaynes sent the e-mails with non-existent domains which did not correspond to the sending IP addresses.

<sup>2</sup> Computers may be identified by their unique IP address number, which consists of blocks of numerals separated by periods.

Jaynes moved to dismiss the charges against him on the grounds that the statute violated the dormant Commerce Clause, was unconstitutionally vague, and violated the First Amendment. The circuit court denied that motion.

During trial, evidence demonstrated that Jaynes knew that all of the more than 50,000 recipients of his unsolicited e-mails were subscribers to AOL, in part, because the e-mail addresses of all recipients ended in "@aol.com" and came from discs stolen from AOL. Jaynes' e-mails advertised one of three products: (1) a FedEx refund claims product, (2) a "Penny Stock Picker," and (3) a "History Eraser" product.<sup>3</sup> To purchase one of these products, potential buyers would click on a hyperlink within the e-mail, which redirected them outside the e-mail, where they could consummate the purchase. Jaynes operated his enterprise through several companies which were not registered to do business in North Carolina, and evidence was introduced as to billing and payment activities for these companies, including evidence that registration fees were paid to AOL with credit cards held by fictitious account holders.<sup>4</sup>

---

<sup>3</sup> Although Jaynes advertised only three products, he created false sender information for each e-mail, using thousands of different IP addresses, user names and website links.

<sup>4</sup> Jaynes' enterprises were apparently quite successful. Although not introduced as evidence during the guilt stage of the trial, counsel for the Commonwealth informed the Court following the jury verdict against Jaynes and during the discussion of bond for Jaynes that Jaynes' "[p]ersonal financing

While executing a search of Jaynes' home, police discovered a cache of compact discs (CDs) containing over 176 million full e-mail addresses and 1.3 billion e-mail user names. The search also led to the confiscation of a storage disc which contained AOL e-mail address information and other personal and private account information for millions of AOL subscribers. Police also discovered multiple storage discs which contained 107 million AOL e-mail addresses. Richard Rubenstein, manager of technical security investigations at AOL, testified that the discs recovered at Jaynes' home "contained proprietary information" of "pretty near all" AOL account customers.<sup>5</sup> The AOL user information had been stolen from AOL by a former employee and was in Jaynes' possession.

Dr. John Levine, a consultant and author, testified as an expert witness and explained that the e-mails sent by Jaynes were not consistent with solicited bulk e-mail, but rather constituted unsolicited bulk e-mail (sometimes referred to as "spam" e-mail) because Jaynes had disguised the true sender and

---

statement list[s] assets at \$17 million and a net worth of \$24 million," and his income from all of his businesses exceeded \$1 million in 2001, 2002 and 2003.

<sup>5</sup> The data on the disc contained, among other things, "a raw dump of the AOL member database" which "contains information about [AOL] subscribers, how they choose to be billed, their e-mail address, specific AOL data fields such as an account number, things of that nature."

header information and used multiple addresses to send the e-mails. He explained:

[H]ere the [e-mail] has been spread around nearly a thousand addresses. Where it's reasonable that you might use maybe a dozen addresses if you have a really big system and you're sending it from a dozen computers, I can't think of a valid reason why you would need to spread your e-mail over a thousand different addresses unless, again, you're trying to disguise the source.

The fact - both the fact that the domains do not seem plausible, they don't seem familiar, and the fact that it's spread out in a way that seems intended to disguise the origin of the mail, is what tells me this is not solicited e-mail.

AOL, which houses all of its e-mail servers in Virginia, was directly affected by Jaynes' spam e-mail attack.<sup>6</sup> Brian Sullivan, the senior technical director for mail operations at AOL, testified that bulk e-mail "tends to create a lot of confusion" for AOL customers and that AOL receives "7 to 10 million complaints per day" regarding spam e-mails. Sullivan also described the impact of spam e-mails, explaining that "[i]f someone's mailbox is full because they got a truckload of spam and there's no more room, a message coming from Grandma is returned back to the sender. We can't take it at that point."

A jury convicted Jaynes of three counts of violating Code § 18.2-152.3:1, and the circuit court sentenced Jaynes to three

---

<sup>6</sup> At trial, evidence demonstrated that all of AOL's servers were located in Virginia, although some were located in Loudoun County and others were located in Manassas.

years in prison on each count, with the sentences to run consecutively for an active term of imprisonment of nine years. The Court of Appeals affirmed his convictions, Jaynes v. Commonwealth, 48 Va. App. 673, 634 S.E.2d 357 (2006). We awarded Jaynes an appeal.

## II. ANALYSIS

Jaynes makes four distinct assignments of error to the judgment of the Court of Appeals. First, he assigns error to the determination that the circuit court had jurisdiction over him on the crimes charged. Second, Jaynes contends Code § 18.2-152.3:1 "abridge[s] the First Amendment right to anonymous speech," and it was error not to reverse his convictions on that basis. Separately, Jaynes assigns as error the failure of the Court of Appeals to hold that Code § 18.2-152.3:1 is void for vagueness. Lastly, Jaynes posits that the statute violates the Commerce Clause of the United States Constitution.

### A. Jurisdiction

Jaynes asserts that the Court of Appeals erred in holding that the circuit court had jurisdiction over him for violating Code § 18.2-152.3:1 because he did not "use" a computer in Virginia. He contends that a violation of that statute can occur only in the location where the e-mail routing information is falsified. Jaynes maintains that because he only used computers to send the e-mails from his home in Raleigh, North Carolina, he

# **EXHIBIT B**

# Convicted spammer gets nine-year sentence

By Andy McCue

Special to CNET News.com

Published: April 11, 2005 11:17 AM PDT

## Welcome Google user!

More headlines related to "jeremy jaynes %2424 million":

- Can't find a parking spot? Check smartphone
- Week in review: Microsoft seconds Icahn bid
- Microsoft's big bid for Yahoo
- Large solar energy array set for GM in Spain
- More matching headlines »

## Add News.com to Google

Add CNET News.com headlines to your Google homepage or Google reader.

## Tools

- Talkback
- Print
- E-mail
- Share

## Related Stories

Spam conviction overturned March 3, 2005

\$1 million bond set for alleged spammer's freedom November 9, 2004

Virginia files felony spam charges December 11, 2003

## A convicted spammer has been sentenced to nine years in prison for sending more than 10 million junk e-mails a day.

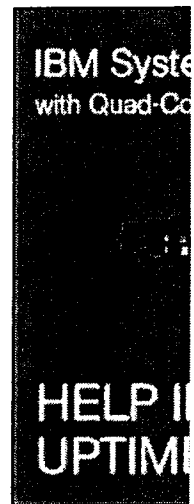
Jeremy Jaynes, also known by his alias, "Gaven Stubberfield," is believed to have raked in between \$500,000 and \$750,000 a month through sales of products via spam. He was rated the eighth most prolific spammer in the world by spam watchdog Spamhaus.

A circuit judge in Loudon County, Va., upheld the sentence recommended by the court when Jaynes was initially convicted last November under a Virginia antispam law, which limits the quantity of bulk e-mail that can be sent and prohibits the use of fake e-mail addresses.

Jaynes, a resident of North Carolina, fell afoul of the law by routing the spam through servers located in Virginia, which disguised the origin of the e-mails. He was also found in possession of a stolen database of 84 million America Online e-mail addresses. He is the first person in the United States to face prison time for spamming.

But the judge delayed the start of the jail term pending an appeal by Jaynes, who is currently out on \$1 million bail.

Jaynes' sister was also found guilty of being an accomplice and fined \$7,500, but the judge dismissed her conviction. Another associate, Richard Rutkowski, was acquitted.



## RSS Feeds

Add headlines homepage or f

More feeds ava

## Today's Top

Steve Wozniak

Microsoft cuts

Google, Viacon records

The iPhone, ta

Apple iPhone v

## Most Popular

The iPhone, ta

Microsoft's fir

The trial revealed some details about the business of spamming. Jaynes used 16 high-speed Internet connections to peddle various fake goods and services, including a Web-history eraser and a stock-picking computer program. Prosecutors claim Jaynes raked in up to \$24 million in sales, some of which he invested in a restaurant and a chain of gyms.

*Andy McCue of Silicon.com reported from London.*

Microsoft vis-a  
ZoneAlarm up  
My night as an

## More from News.com on this story's topics

### Lawsuits

Create an email alert | RSS feed

### Spam and phishing

Create an email alert | RSS feed

### Legal

Create an email alert | RSS feed

### See more CNET content tagged:

spamming, spammer, sentence, Virginia, e-mail address

**ADD A COMMENT** (Log in or register)

4 comments (Page 1 of 1)

#### Spamhaus sucks

by System Tyrant April 11, 2005 11:44 AM PDT

I have a real problem with the way Spamhaus does business. Their method of blocking IP address is a bad way to stop spammers. For people like me who use a shared web host we get our e-mails blocked as well. I don't like spammers any more than anybody else, but their method cost me money. I personally think they are a bunch of arrogant b\*\*\*\*\*s who should be shut down or better regulated. I personally will never knowingly use an ISP or webhost that uses Spamhaus services.

For those who think Spamhaus is great you might want to know that they are a UK company that states over and over on their site that they can't be sued. They also say they don't care about who it hurts as long as it stops spammers. I really hope that CNET will do a story on them.

I think when people know and understand the damage they can inflict on good users and businesses they won't find their service to be so great. They can cost small business such as the one I work at thousands of dollars a day and their is little to no recourse we can take. If they were in the US they would be out of business by now.

[Reply to this comment](#) | [View reply](#)

Markets  
Market n  
filings, a

### Related quotes

Dow Jones  
Industrials

S&P 500

NASDAQ

CNET TECH

Ente

# SOPHOS

Global websites | Press | Co

11 April 2005

## \$24 million spammer sentenced to 9 years in jail, Sophos reports

A US court has sentenced Jeremy Jaynes, 30, to 9 years in jail for sending emails with fraudulent and untraceable routing information.


Jaynes used bulk spam email to market fake products such as a "Fedex refund processor" for \$39.95. This product was supposedly capable of helping people working from home earn \$75 an hour. In one month alone, Jaynes received orders for the product totalling almost \$400,000.


Jaynes, who sometimes used the pseudonym Gaven Stubberfield, is said to have built up a fortune of \$24 million selling products via spam.

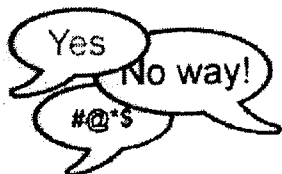
"This sentence sends out a strong message to other spammers that their activities are not going to be tolerated by the US authorities," said Graham Cluley, senior technology consultant for Sophos. "Those involved in spamming would be sensible to take heed of Jaynes's predicament, and close down their spam operations. It's likely that Jeremy Jaynes's nine year sentence will keep a few spammers awake at night wondering if the rewards are really worth it."

Sophos recommends companies protect themselves with a consolidated solution which can defend against the threats of both spam and viruses.

 Bookmark with del.icio.us

 Submit this story to digg

 Submit this story to slashdot



Have your say!

### When considering your anti-malware security vendor, what is more important to you?

- Speedier protection against threats
- More detailed description of what the threat does
- Both are equally important

Submit 

#### See also:

- > Best practice advice for minimising exposure to spam
- > Sophos PureMessage - protecting your email servers and gateways against spam and viruses
- > White papers about spam



spamfo.co.uk

search... Submit

Log In » Create Account

Ads by Google

Stop Paper Junk Mail

Prevent unsolicited mail at home. It's free! www.ProQuo.com

Email Spam Filters (free)

Eliminate Spam. Protect Yourself Nothing to install - start now www.Silverfeed.com

Blacklist Checker Pro?

Check Your IP, Receive Removal Info Instant Notification - Free Trial! BlackListMonitor.com

Spam and Virus Free Email

Our System Blocks Virus and Spam Register domain Free with Hosting www.BlackSun.ca/

Syndicate

Buttons for RSS 0.91, RSS 1.0, RSS 2.0, ATOM 0.3, and OPEN SHARE IT!

How Jeremy Jaynes earned \$750k per month for spamming

Chris Hunter Monday, 15 November 2004

Recently, the prolific spammer jeremy jaynes received a 9 year sentence for spamming, this article by the associated press digs a bit deeper...

\* UPDATE - 10TH APRIL - Jeremy Jaynes gets nine years\*

Jaynes' business was remarkably lucrative; prosecutors say he grossed up to \$750,000 per month. If you have an e-mail account, chances are Jaynes tried to get your attention, pitching software, pornography and work-at-home schemes.

The eight-day trial that ended in his conviction this month shed light on the operations of a 30-year-old former purveyor of physical junk mail who worked with minimal assistance out of a nondescript house in Raleigh, N.C.

A state jury in Leesburg has recommended a nine-year prison term in the nation's first felony trial of spam purveyors. Sentencing is set for February.

During the trial, prosecutors focused on three products that Jaynes hawked: software that promises to clean computers of private information; a service for choosing penny stocks to invest in; and a "FedEx refund processor" that promised \$75-an-hour work but did little more than give buyers access to a Web site of delinquent FedEx accounts.

Jaynes, going by Gaven Stubberfield and other aliases, had established a niche as a pornography purveyor, said Assistant Attorney General Russell McGuire, who prosecuted the case. But Jaynes was constantly tweaking and rotating products.

Relatively few people actually responded to Jaynes' pitches. In a typical month, prosecutors said during the trial, Jaynes might receive 10,000 to 17,000 credit card orders, thus making money on perhaps only one of every 30,000 e-mails he sent out.

But he earned \$40 a pop, and the undertaking was so vast that Jaynes could still pull in \$400,000 to \$750,000 a month, while spending perhaps \$50,000 on bandwidth and other overhead, McGuire said.

"When you're marketing to the world, there are enough idiots out there" who will be suckered in, McGuire said in an interview.

Prosecutors believe Jaynes had a net worth of up to \$24 million, and they described one of his homes as a mansion, though the e-mail came from a house described as average.

Jaynes got lists of e-mail addresses millions of them through a stolen database of America Online customers. He also illegally obtained e-mail addresses of users of the online auction site eBay.

Prosecutors don't know how he got the lists, though McGuire said the AOL names matched a list of 92 million addresses an AOL software engineer has been charged with stealing. However Jaynes got them, they were particularly valuable because AOL customers and eBay users by their very nature have already shown a willingness to engage in e-commerce.

Under Virginia law, like a federal anti-spam measure that took effect months later, sending out