The National Association of Criminal Defense Lawyers and the Electronic Frontier Foundation write in response to the Commission's request for public comment about on the implementation of Section 4(b) of the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (the "CAN-SPAM Act of 2003"), Pub. L. 108-187, which directs the Commission to review and as appropriate amend the sentencing guidelines and policy statements to establish appropriate penalties for violations of 18 U.S.C. §1037 and other offenses that may be facilitated by sending a large volume of e-mail. We thank the United States Sentencing Commission for the opportunity to offer comment.

Interests of the Commentators

The **National Association of Criminal Defense Lawyers** (NACDL) is the preeminent organization in the United States advancing the mission of the nation's criminal defense lawyers to ensure justice and due process for persons accused of crime or other misconduct. A professional bar association founded in 1958, NACDL's more than 10,400 direct members -- and 80 state and local affiliate organizations with another 28,000 members -- include private criminal defense lawyers, public defenders, active U.S. military defense counsel, law professors and judges committed to preserving fairness within America's criminal justice system.

The National Association of Criminal Defense Lawyers (NACDL) encourages, at all levels of federal, state and local government, a rational and humane criminal justice policy for America -- one that promotes fairness for all; due process for event the least among us who may be accused of wrongdoing; compassion for witnesses and victims of crime; and just punishment for the guilty.

Equally important, a rational and humane crime policy must focus on the social and economic benefits of crime prevention -- through education, economic opportunity, and rehabilitation of former offenders. As a society, we need to eschew such simplistic, expensive, and ineffective "solutions" as inflexible mandatory sentencing, undue restriction of meritorious appeals, punishment of children as adults, and the erosion of the constitutional rights of all Americans because of the transgressions of a few.

NACDL's values reflect the Association's abiding mission to ensure justice and due process for all.

The **Electronic Frontier Foundation** ("EFF") is a non-profit, civil liberties organization founded in 1990 that works to protect rights in the digital world. EFF is based in San Francisco, California, but has members all over the United States.

EFF has been deeply concerned about the criminalization of online behavior since its inception. The founders intended EFF to bring balance and reason to law enforcement in cyberspace. One incident that brought this need home was a 1990 federal prosecution of a student for publishing a stolen document. At trial, the document was valued at $79,000. An expert witness, whom EFF helped locate, was prepared to testify that the

document was not proprietary, and was available to the public from another company for $13.50. When the government became aware of this information through defense's cross-examination of government witnesses, it moved to dismiss the charges on the fourth day of the trial.

Accordingly, EFF is very concerned that the Sentencing Commission act very carefully with regard to computer crime sentencing. We believe that those convicted of computer-related crimes are already punished more harshly compared to other crimes for the reasons stated in these Comments.

COMMENTS

Congress has asked the Commission to review and revise where necessary the sentencing guidelines to fashion appropriate sentencing for violators of 18 U.S.C. §1037. The commentators believe that the proposed guidelines and enhancements risk over-punishing violators through overly severe and, at times, duplicative sentencing. CAN-SPAM violations are dissimilar and far less harmful than many of the criminal offenses referenced to §§2B1.1 and 2B2.2. Moreover, many of the proposed enhancements effectively raise the base offense level or "re-punish" exacerbating elements that are already included in the offense conduct or addressed by other sentencing enhancements. The commentators urge the Commission to consider these important issues in adopting appropriate sentencing guidelines.

I. REFERENCING SECTION 1037 OFFENSES TO GUIDELINE 2B1.1 OR 2B2.2 WOULD RESULT IN PUNISHMENT DISPROPORTIONATE TO THE CRIME

A. Section 1037 offenses are less harmful than other crimes referenced to the same guidelines.

The application of the sentencing guidelines should result in punishment proportionate to the severity of the harm caused. Section 1037 differs from the usual economic fraud case in that the fraud isn't targeted towards obtaining any thing of tangible value. The fraud (mislabeling the origin, etc.) only assists the sender in evading fines under the statute and makes the message less likely to be identified as unwanted email by any filtering software the recipient might have. Also, unlike the more serious offense of computer fraud and trespass under 18 U.S.C. 1030, most spam does not intentionally damage the recipient's system, nor alter, delete, copy or otherwise misuse the recipient's data. More harmful forms of spamming, including those that involve privacy violations and damage to computer systems, are already punishable under 18 U.S.C. 1030(A)(5)(a) or 18 U.S.C. 2701 et. seq. and referenced to 2B1.1.

Because section 1037 fraud is less morally culpable and less harmful than other computer crime, unauthorized access or fraud cases, it should be punished less severely. Congress has indicated that this is the desired outcome by making most section 1037 violations misdemeanors, and those with aggravating circumstances three-year felonies.

Therefore, the commentators are concerned that referencing to 2B1.1 would over punish section 1037 offenses by sentencing them in the identical manner as section 1030 and other economic fraud cases, which are at least five-year felonies.

Similarly, a section 1037 offense is less serious than offenses referenced to guideline 2B2.3 (Trespass). Almost any on-line activity involves sending electrons, possibly unwanted, to networked computers, but most on-line activities are not crimes. Additionally, most spam has only a *de minimus* impact on the recipient's hardware. Unlike other offenses referenced to 2B2.3, section 1037 offenses do not involve physical trespass on an area in which the owner traditionally has an absolute right to exclude. *See, e.g., Intel v. Hamidi*, 30 Cal. 4th 1342 (2003). Since 1037 offenses are not as dangerous as other trespass crimes referenced to this section, which require non-routine intrusions into physical space, *see* 16 U.S.C. 146 (public parks); 18 U.S.C. 2199 (stowing-away on vessels or aircraft); 18 U.S.C. 1857 (driving livestock on public lands), violations should not be sentenced in the same manner.

Therefore, the commentators believe that referencing 2B1.1. or 2B2.3 will overstate the seriousness of the offense, even for more serious violations of section 1037. This concern is amplified for misdemeanor violations of 1037 (a)(2), (3) and other regulatory violations. These should not have the same base offense level as more serious violations.

B. The loss enhancements under the proposed guidelines will produce inconsistent and unjust sentencing for Section 1037 offenses.

Additionally, referencing this offense to the fraud table in 2B1.1 will result in excessive and unpredictable sentencing. Measuring the economic value of "loss" in cases such as those arising under section 1037 involves calculating intangible harm and will result in uncertainty in sentencing. In estimating economic loss, 2B1.1. recommends that judges assess (i) the fair market value of the property taken or destroyed, (ii) the cost of repairs to the damaged property, (iii) the number of victims multiplied by the average loss to each victim, (iv) the reduction that resulted from the offense in the value of equity securities or other corporate assets, and (v) more general factors, such as the scope and duration of the offense and revenues generated by similar operations. These categories of harm described as loss are inapplicable to spamming violations or extremely difficult to quantify in monetary terms. As a result, the loss estimation for identical offenses can differ widely, resulting in grossly disparate sentences for identical conduct. Additionally, the estimation of loss can be manipulated by victims, investigators and prosecutors.

For example, loss of productivity is difficult to measure. In the 2000 denial of service attacks on Yahoo! Inc., the company went off-line for about three hours. Yahoo! initially refused to estimate how much the attack cost it in lost revenue. Yahoo! makes money from sale of goods and from showing advertisements. It is difficult to estimate whether Yahoo! actually lost any sales or advertising contracts as a result. Yet, some analysts estimated that Yahoo!'s loss would add up to millions of dollars. Jennifer Mack, *FBI Talks With Yahoo! About Attack,* ZDNet News, Feb. 7, 2000, *at*

http://zdnet.com.com/2100-11-518359.html?legacy=zdnn. The resulting losses in revenue and market capitalization sustained by five popular websites targeted by the Feb. 2000 denial-of-service attacks allegedly totaled $1.2 billion. Matt G. Nelson, *Report Says Web Hacks to Cost $1.2B*, InformationWeek, Feb.11, 2000, *at* http://www.techweb.com/wire/story/TWB20000214S0006. The attack was perpetrated by a Canadian juvenile who never gained unauthorized access to Yahoo! machines or harmed data on the victim systems. Yet sentencing according to these loss estimates would have resulted in the maximum punishment possible under the law.

Similarly, the mi2g consultancy firm estimated that January 2004's "mydoom" virus cost businesses $38.5 billon. In comparison, the National Climatic Data Center estimates that 2003's hurricane Isabel cost only $4 billion. http://lwf.ncdc.noaa.gov/img/reports/billion/disasters-since-1980.jpg

Of course, loss can be difficult to estimate in any economic crime cases. However, this is a serious problem in section 1037 cases because loss is defined by the victim's conduct rather than by the offender's conduct and commonly involves the valuation of intangibles like employee productivity. As a result, the loose measures of loss undermine uniformity in sentencing. It also means that loss can be a distorted, or even wholly inaccurate, reflection of the defendant's culpability.

We believe that the proposed guidelines for section 1037 would be unworkable. To insure proportionate and just sentencing, the Commission would have to draft a new guideline for this offense, taking the above concerns into consideration.

II. MANY OF THE PROPOSED SENTENCE ADJUSTMENTS EFFECTIVELY RAISE THE BASELINE OFFENSE LEVEL OR DUPLICATE EXISTING ADJUSTMENTS ADDRESSING THE SAME AGGRAVATING FACTORS.

A. The proposed victim and mass marketing enhancement provisions effectively increase the base offense level of section 1037 violations and therefore over-punish the offense.

Unsolicited commercial e-mail clearly produces more harm if sent to more users. Application of the enhancement at §2B1.1(b)(2)(A)(I), however, does not merely distinguish and more severely punish high-volume spamming, but rather increases the base offense level by two for any and every violation. All spam is sent to 10 or more recipients, and thus all violations would have 10 or more victims. As a result, the base offense level becomes 8 – higher than crimes involving stolen property or property damage – and disproportionate to the violation.

The mass marketing adjustment at §2B1.1(b)(2)(A)(ii) is similarly duplicative. As above, application of this adjustment merely increases the base offense level by 2. CAN SPAM by definition punishes mass marketing. The statute criminalizes certain

transmissions of "multiple *commercial* electronic mail messages," and therefore addresses the "plan[s], program[s], promotion[s] or campaign[s] to induce a large number of persons to purchase goods or services …" that the factor targets.

A properly calibrated guideline could better serve the aim of distinguishing severe spamming from milder forms. Recent spamming litigation provides a guide to scaling multiple victim adjustments. In a recent case, AOL won a suit against National Health Care Discount for sending an estimated 126 million unsolicited e-mails to AOL users over a 30-month period. (The court found that NHCD had sent 150 million additional e-mails to non-AOL subscribers over the same period.) *America Online v. Nat'l Heath Care Discount*, 174 F. Supp. 2d 890 (N.D. Iowa 2001). In another case, Earthlink successfully sued an individual that had sent 1 million spam messages per day from 343 stolen accounts, with an average life span of 2.5 days per account, for a total of 857.7 million unsolicited commercial e-mails. *Earthlink v. Carmack*, Civ. Action File. No. 1:02-CV-3041-TWT (N.D. Ga. 2003). As alternative reference points, services that mail spam messages regularly set rates by each million mailed and commercial vendors such as Data Resource sell lists containing 85 million e-mail addresses. *See* David Steitfield, *Opening Pandora's In-Box*, L.A. Times, May 11, 2003, at 1. A fairer guideline would increase the offense level only if the number of illegal messages sent is in the many, many millions.

Importantly, though a sentence enhancement based on the number of victims risks duplicating the economic loss enhancements at §2B1.1(b)(1), it may represent a fairer measure of culpability than an economic loss adjustment based on the valuation of intangibles. Pecuniary harm will rise in proportion to the number of victims. An economic loss adjustment, however, would result in unpredictable sentencing because of the estimation difficulties identified above. An appropriate multiple victim adjustment would be more readily measured, more consistent and therefore more just.

B. A sophisticated means enhancement may be appropriate if the level of sophistication triggering the factor is set appropriately high.

An upward adjustment for the use of "sophisticated means" may deter section 1037 violations that are particularly difficult to trace. This, in turn, may help promote the economy of law enforcement resources. The guidelines should be careful, however, to set the level of sophistication deserving of sentence adjustment at an appropriately high level. All CAN-SPAM violations will inherently involve a level of computer sophistication beyond the level of the average person. The guidelines should discourage higher sentences when the means employed are those required to conduct the anonymous mass distribution of e-mail.

C. An "improper means" enhancement increases the base offense level while punishing behavior not clearly deserving of more severe sentencing.

This enhancement would effectively raise the base offense level for 1037 violations, as most violators will obtain e-mail addresses using the methods identified.

The only other source for email addresses would be commercial email list vendors. There is little guarantee that the list vendors themselves did not obtain their e-mail lists through harvesting, trickery or outright fraud and driving spammers to use commercially available e-mail lists may have the unintended effect of making these commercial vendors more economically viable. Second, it is unclear whether certain forms of e-mail address harvesting are indeed improper. A harvester simple collects publicly available e-mail addresses in the same way a conventional mass mailer might stroll down a residential street to collect mailing addresses. The commentators do not believe that a violator is more culpable for having collected published email addresses from web pages than for having purchased a list from another party. There is no compelling reason to treat addresses available on public websites or message boards differently from commercial email lists or the collection of publicly observable residential addresses.

D. Sentencing under section 5(d)(1) of the Act for the transmission of sexually oriented materials should not be referenced to guidelines for child pornography or obscenity because sexually oriented materials that are not child pornography or obscenity are protected by the First Amendment. Additionally, the Commission should be wary of duplicating existing enhancements under the sentencing guidelines for the underlying offense.

Child pornography and obscenity are only a fraction of sexually oriented materials. Most "sexually oriented materials" under section 5(d)(1) of the CAN SPAM Act are First Amendment protected, completely legitimate to possess and distribute, and may have socially beneficial purposes. The Commission absolutely should not sentence mislabeling these free speech materials in the same manner as distributing illegal child pornography or obscenity.

In the rare cases where someone violates section 5(d)(1) by transmitting these illegal materials by spam, and only in these cases, the Commission should reference the guidelines applicable to those underlying offenses.

In doing so, the Commission can rest assured that the current guideline scheme adequately punishes any extra harm for the volume of illicit materials transmitted by spam. For example, child pornography crimes, which are punishable under 18 U.S.C. 2252, are referenced to guidelines 2G2.2 and 2G2.4. Guideline 2G2.2 provides for upward adjustments whenever a violator uses a computer to transmit, receive, distribute or advertise the illegal material. U.S.S.G. 2G2.2(5). The guideline increases the offense level in proportion to the number of illicit images involved. U.S.S.G. 2G2.2(6)(A)-(D). Guideline 2G2.4 contains similar provisions based on the number of illegal media possessed (U.S.S.G. 2G2.4(2)); whether possession occurred on a computer (U.S.S.G. 2G2.4(3)); and on the number of images (U.S.S.G. 2G2.4(5)(A)-(D)). Additionally, the sexual exploitation of children, punishable under 18 U.S.C. 2261, references guidelines that recommend duplicative adjustments. See e.g. U.S.S.G. 2G2.2. As in the child pornography crimes, the applicable guideline calls for an increased offense level based on the number of images, which effectively duplicates the upward adjustments of

2B1.1(b)(2)(A)-(B). Therefore, to the extent that a defendant violates section 5(d)(1) of the act by transmitting child pornography or obscenity, existing guidelines cover such conduct adequately without need for additional enhancements.

III. CONCLUSION

We encourage the Commission to act carefully in formulating appropriate sentencing for violations of the CAN-SPAM Act. Such violations do not inflict nearly the same level of harm, involve the same degree of privacy invasion, or constitute the same seriousness of fraud as do other criminal offenses referenced to the guidelines suggested in the Commission's Request for Comment. We therefore urge the Commission to develop new guidelines in light of the concerns above. The current proposal, as we see it, is fraught with duplicative and overly severe treatment of the offense. A fairer proposal must give adequate consideration to the unique nature of this new crime.

Dated: March 17, 2004

Respectfully Submitted,

By: _____

Jennifer Stisa Granick, California Bar No. 168423
Center for Internet and Society
Cyberlaw Clinic
559 Nathan Abbott Way
Stanford, CA 94305-8610
Tel. (650) 724-0014
Counsel for Commentators

Carmen D. Hernandez, Co-Chair
Sentencing Guidelines Committee
National Association of Criminal Defense Lawyers
One Columbus Circle, N.E.
Suite G-430
Washington, D.C. 20544

Lee Tien, Senior Staff Attorney
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110