
Public Comment



Proposed Amendments

2004
VOLUME II

THE SECRETARY OF STATE
WASHINGTON

February 25, 2004

To the Sentencing Commission:

I want to thank you for considering the proposal to enhance sentencing guidelines for violations of our passport and visa fraud laws. Ensuring the security of our borders and protecting the safety and security of American citizens at home and abroad are the highest priorities for the Department of State. Maintaining the integrity of U.S. passports and visas is a critical component of our global effort to fight terrorism, in addition to ensuring that our immigration policies and laws are enforced.

A U.S. passport establishes U.S. citizenship and identity, making it the most widely accepted and versatile identity document in the country. It is considered the "gold standard" of all passports and is used by our citizens not only to visit foreign countries and enter the United States, but also domestically to establish bank and credit card accounts, cash checks, apply for a driver's license, apply for welfare or unemployment, and to conduct activities that require proof of U.S. citizenship. Similarly, visas are highly sought after because they allow the bearer to request legal entry into the United States.

Investigations of passport and visa fraud are a vital part of strong border and homeland security procedures. I believe these new guidelines will be a clear signal that the United States Government recognizes the severity of passport and visa fraud and the importance of maintaining our border security. Ambassador Francis Taylor, Assistant Secretary for Diplomatic Security, will address our specific proposal with you in a separate letter. Thank you for your consideration on this important matter.

Sincerely,



Colin L. Powell

The U.S. Sentencing Commission,
One Columbus Circle, N.E.,
Suite 2-500, South Lobby,
Washington, D.C. 20002-8002.



United States Department of State

*Assistant Secretary of State
for Diplomatic Security*

Washington, D.C. 20520

FEB 25 2004

To All Members of the Commission:

The Department of State and the Bureau of Diplomatic Security's (DS) role to investigate and seek prosecution of those committing passport and visa fraud has increased in the post-9/11 environment. In order to further strengthen our efforts, I believe we need federal sentencing guidelines that are appropriate for the crimes.

While the DS sentencing initiative before you addresses crimes related to the users of false and fraudulently obtained passports and visas, we fully intend to work with the Commission during the next term to propose raising the sentences for crimes relating to the vendors of said documents (falling under Federal Sentencing Guidelines 2L2.1). We strongly believe that higher sentences for those responsible for the illegal sale of passports, visas, and supporting documents is a logical next step in our homeland security efforts.

Likewise, with the integrity of passports and visas at the core of U.S. border security efforts, someone who has obtained a U.S. passport or visa and/or uses a false passport or visa, is obstructing the homeland security efforts of the United States. In the U.S. judicial system, someone convicted of a similar false statement before law enforcement or judicial officials (18 USC 1502, 1505-13, or 1516) would face a base offense level of 14 under current Federal Sentencing Guidelines (2J1.2).

The goal of the Department of State is to achieve sentencing levels appropriate for those individuals convicted of violations of passport or visa fraud. Given the overwhelming importance of the integrity of U.S. passports and visas in the post-9/11 environment, I believe we can obtain these appropriate sentencing levels with a combination of well-defined specific offense characteristics and a slight increase in the base offense level.

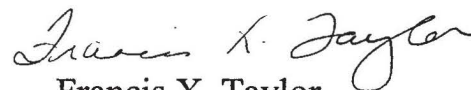
The U.S. Sentencing Commission,
One Columbus Circle, N.E.
Suite 2-500, South Lobby
Washington, D.C. 20002-8002

Attached are my comments on the specific issues before the Commission. These comments are meant to clarify and, in some cases, expand on our previously submitted material. Please note that our goal in focusing on Specific Offense Characteristics, as opposed to seeking an overall major increase in the base offense level, is to have guidelines that appropriately address different levels of violations of law related to passport and visa fraud. Individuals who apply for U.S. passports using false and fraudulent information, however, should face an increased sentence. The two primary reasons are that they are already in the United States (in the case of passport applications), having entered illegally or overstayed their legal entry time limit, and are attempting to hide their true citizenship and/or identity to obtain a genuine passport or visa. Finally, someone who applies for a U.S. passport or visa using false statements and is successful in obtaining the documents, should face the stiffest of the penalties.

If the current Federal Sentencing Guidelines for passport and visa fraud are adjusted to the levels indicated above, I believe that future sentences for convictions of these crimes will provide the appropriate deterrence and punishment. With increased sentences, the special agents of the Diplomatic Security Service will have the leverage necessary to enlist the assistance of defendants to identify persons involved in the manufacture and/or sale of illegal citizenship and identity documents, both inside and outside the United States. Further, once federal judges start handing out prison sentences for these crimes, the deterrent effect will reduce the overall number of people inclined to commit these offenses.

On behalf of the Department of State and Bureau of Diplomatic Security, thank you for your efforts and assistance in this matter. I stand committed to this initiative and welcome any further questions from the Commission.

Sincerely,



Francis X. Taylor
Ambassador

Attachment: Proposed Changes to Sentencing Guidelines

Proposed Changes to Sentencing Guidelines

§2L2.2. Fraudulently Acquiring Documents Relating to Naturalization, Citizenship, or Legal Resident Status for Own Use; False Personation or Fraudulent Marriage by Alien to Evade Immigration Law; Fraudulently Acquiring or Improperly Using a United States Passport

(a) Base Offense Level: ~~8~~[8-12]

DS COMMENT: (Raise to 9, keeping the base 2 levels below 2L2.1)

(b) Specific Offense Characteristics

(1) If the defendant is an unlawful alien who has been deported (voluntarily or involuntarily) on one or more occasions prior to the instant offense, increase by ~~2~~[4] levels.

DS COMMENT: (Leave as 2)

(2) If the defendant committed any part of the instant offense after sustaining (A) a conviction for a felony immigration and naturalization offense, increase by ~~2~~[4] (**4**) levels; or (B) two (or more) convictions for felony immigration and naturalization offenses, each such conviction arising out of a separate prosecution, increase by ~~4~~[6] (**6**) levels.

DS COMMENT: (Make a conviction under scenario (A) a level 4 and (B) a level 6, providing for appropriate level increases based on the increasing seriousness of the acts)

(3) If the defendant was a fugitive wanted for a felony offense in the United States, [or any other country,] increase by [4-10] levels.

DS COMMENT: (If wanted for a crime of violence or controlled substance increase by 8 levels; if wanted for any other felony crime increase by 4 levels. This mirrors similar enhancements in the current guidelines.)

[~~(4) If the defendant fraudulently obtained or used a United~~

States passport, increase by [2-8] levels.]

DS COMMENT: (In place of this proposed language insert: used a counterfeit or forged passport or visa increase by 4 levels; if the defendant fraudulently applied for a U.S. passport or visa increase by 6 levels; if the defendant used a fraudulently obtained U.S. passport or visa increase by 8 levels.)

Drafted: DS/MFO:Mike Johnson/DS/BFOClaude Nebel
Cleared: DS/FLD: Wdeering ok
DS/DO: TmcKeever ok
DS/DSS: JMorton

TO:

Public Affairs Office
United States Sentencing Commission
Suite 2-500
One Columbus Circle NE
Washington, DC 20002

I. INTRODUCTION:

The United States Sentencing Commission has requested public comment regarding implementation of Public Law 108-187, the CAN-SPAM Act of 2003. 69 F.R. 2169 (14 January 2004). This commentary is submitted accordingly.

II. COMMENTATOR'S BACKGROUND & CONTACT INFORMATION:

Background: The Commentator, Kenneth H. Ryesky, Esq., is an attorney at law in East Northport, NY, and is an Adjunct Assistant Professor, Department of Accounting and Information Systems, Queens College of the City University of New York.

Contact Information: Kenneth H. Ryesky, Esq., P.O. Box 926, East Northport, NY 11731. Telephone: 631/266-5854 (vox), 631/266-3198 (fax). E-mail: khresq@sprintmail.com.

Disclaimer: The comments herein reflect the Commentator's personal views, and do not necessarily represent the official position of any organization or institution with which the Commentator is or has been associated, affiliated, employed or retained.

III. CLASSIFICATION OF NEW OFFENSES:

Violations of 18 U.S.C. § 1037 have attributes germane to, inter alia, USSG § 2B1.1 (Fraud, Theft, and Property Destruction), and USSG § 2B2.3 (Trespass). It would serve well to basically classify these new offenses under USSG § 2B1.1, for the harms typically associated with such offenses entail diminution of the victims' data storage capacity, whether in the victims' personal computers or in the victims' e-mail accounts, and also entail quantifiable and unquantifiable expenses out of the pockets of the e-mail recipients, the enforcement authorities, and society as a whole. As more fully discussed below, appropriate tie-in with USSG § 2B2.3 trespass-type attributes of the offense should be accomplished through enhancements, where appropriate. The base level of the offense should vary with the seriousness of the offense.

IV. SOPHISTICATED MEANS:

The use of computer technology has a certain degree of complexity, and is commonly thought of as a "sophisticated means" of committing offenses. But some uses are more "sophisticated" than others. The "sophisticated means" entailing falsification of entities, identities and locations, such that detection of, apprehension of, or information concerning the perpetrator is clearly contemplated in USSG § 2B1.1(b)(8). The law enforcement authorities, the recipients of the illegal e-mails, and the administrators of the systems through which the illegal e-mails are transmitted all have the need and the right to know the identity and whereabouts of the perpetrator. The § 2B1.1(b)(8) enhancements are most relevant to the new offenses set forth in 18 U.S.C. § 1037 and other provisions of Public Law 108-187, and should be applied thereto.

V. ENHANCEMENTS:

Certain factors cause violations of 18 U.S.C. § 1037 to be especially egregious, harmful and destructive. Enhancements should be provided in such instances, including but not limited to the following:

A. The violator knew or should have known that the recipient specifically objected or would object to the receipt of the unsolicited e-mail. This is especially relevant where the violator failed to act upon one or more victims's opting out under 15 U.S.C. § 7704(a)(5), or any "Do Not E-Mail" registry that may be established pursuant to 15 U.S.C. § 7708 or otherwise.

B. The E-mail involved was particularly large, lengthy or capacious. Inasmuch as many e-mail users' accounts entail kilobyte capacity limitations, the use of an e-mail message of 100 KB is more obviously egregious than the use of an e-mail message of 1 KB. There should be a graduated scale of enhancements for size of the illegally-transmitted message involved. As an example, a message of 5 or more KB should warrant a 1 level enhancement; 10 KB, 2 levels; 20 KB, 3 levels; 50 KB, 4 levels; 100 KB, 5 levels; 200 KB, 6 levels. The size of the message should include any attachments. Serial messages should be aggregated together for the purpose of this enhancement. An unsolicited message transmitted from the same sender to the same recipient address within 24 hours or less after a previous message should be considered a serial message for the purpose of aggregating the messages for this enhancement.

C. The E-mail involved a virus. The use of e-mail to spread viruses has already been amply demonstrated to cause global damage. An e-mail sent in violation of 18 U.S.C. § 1037 that also contains a computer virus, or otherwise intentionally facilitates the spread of a computer virus, is particularly egregious, and warrants an enhancement of at least 6 levels.

D. The e-mail involved wrongfully used a trademark, trade name, or other intellectual property. Many deceptive e-mails improperly use trademarks, trade names or other intellectual property, including names of proprietary pharmaceuticals, corporations, publications or websites. This warrants some sort of enhancement, especially where the rightful owner of the intellectual property has previously objected. Unfortunately, many intellectual property owners such as pharmaceutical manufacturers have not taken a proactive stance against the use of their trademarks and trade names, obviously finding some positive benefit from the negative publicity.

Pfizer's reluctance to go after those who use its proprietary name "Viagra" is one example. Though Pfizer, in this example, may derive benefit from the bandying about of the name of its drug on the streets and in cyberspace, the public is harmed where the product being purveyed is not actually Pfizer's product as implicitly claimed. Accordingly, some enhancement for the wrongful use of a trademark, trade name or other intellectual property should apply even where the owner of the intellectual property has been less than zealous in protecting its rights.

E. The recipient's conduct realized income or revenue that was improperly omitted from a tax return. Under the American taxation system, which depends upon members of the public complying without being compelled to do so by action of a government agent, there is a strong imperative that the tax laws be enforced, lest the public sentiments wax cynical and the voluntary compliance deteriorate. The public needs to see that there are negative consequences for failing to comply with the tax laws. Accordingly, any violation of 18 U.S.C. § 1037 is aggravated where the defendant has received money or other property in the course of his or her conduct and has failed to pay his or her legal share of the taxes imposed upon the transaction. Moreover, the knowledge that one's violation of 18 U.S.C. § 1037 may carry greater penalties where there has been a tax violation in the process can be expected to help induce voluntary tax compliance, even if such compliance comes about after detection of the 18 U.S.C. § 1037 violation, but before the deadline for filing the tax return. There should be an enhancement where the conduct involving the illegal e-mail also entailed a tax violation or a tax loss to the government, whether or not the violator was also prosecuted for Internal Revenue Code or state tax code violations. Such enhancements should be commensurate with the tax loss involved, and in consonance with the Tax Table set forth in USSG §2T4.1.

F. The defendant improperly obtained the e-mail address(es). This includes, but is not necessarily limited to, harvesting of e-mail addresses from the users of a Web site, proprietary service, or other online public forum without authorization and the random generating of e-mail addresses by computer; or knew that the commercial e-mail messages involved in the offense contained or advertised an internet domain for which the registrant of the domain had provided false registration information.

G. The illegal e-mail consisted of or contained sexually-oriented material. This is obviously a most aggravating factor, for which an enhancement is surely warranted. Children are especially vulnerable victims of pornography, accordingly, enhancement of the sentence is especially warranted where one or more children were the recipient.

H. The conduct entailed the transmission of a large volume of unlawful e-mail. There should be a graduated scale of enhancements, according to the volume of e-mail sent in the course of the conduct. 18 U.S.C. § 1037 is couched in terms of "multiple" electronic mail messages, and, with respect to § 1037, subparagraph 1037(d)(3) defines "multiple" with respect to electronic mail messages as more than 100 electronic mail messages during a 24-hour period, more than 1,000 electronic mail messages during a 30-day period, or more than 10,000 electronic mail messages during a 1-year period. There are, however, other provisions of the Can Spam Act that can be violated with a single e-mail message, including, for example, 15 USCS § 7704(d), which requires that sexually oriented material be labeled as such in the subject heading. With respect to such other provisions, initial the threshold for "a large volume" of unlawful e-

mail should be, if not lower, at the standard set forth in 18 U.S.C. § 1037(d)(3). Further enhancements should obtain at other thresholds beyond the initial, e.g., 2 level enhancement for more than 100 messages in a 24-hour period, 3 level enhancement for more than 250 messages in a 24-hour period, 4 level enhancement for more than 500 messages in a 24-hour period, et cetera.

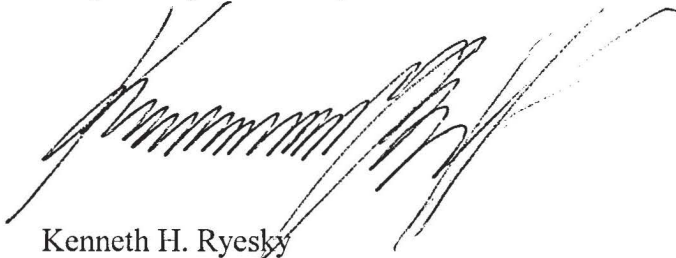
I. The conduct entailed the violation of other federal or state laws. Some "spam" e-mails are sent in the course of conduct that violates other laws. In addition to the taxation issues discussed in Paragraph E above, unsolicited e-mail has been known to contravene, inter alia, the 39 U.S.C. § 1302 prohibition against chain letters scams, or the illegal prescription and dispensation of medications. These all are aggravating circumstances that warrant enhancement of the level of the offense for sentencing purposes.

VI. CONCLUSION:

The transmission of unlawful electronic mail is a serious crime because it imposes vast financial and social burdens upon society as a whole, and upon the recipients of the e-mail, and upon the systems through which the unlawful e-mail is sent. Moreover, unlawful electronic mail is frequently used as a means to facilitate other activities that are wrongful and/or illegal in their own right. The financial transactions done in connection with unlawful electronic mail are frequently hidden and unreported for purposes of tax administration, thus frustrating the tax collection process and imposing additional burden upon the taxpaying public.

Accordingly, it is important to punish those convicted of offenses involving unlawful transmission of electronic mail, and to tailor such punishment to the degree of harm caused, including harm in collateral related areas. Appropriate enhancements to the level of the offense are thus imperative.

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'Kenneth H. Ryesky', written over a horizontal line.

Kenneth H. Ryesky
22 January 2004

Alex Barylo
11114 Greiner Rd
Philadelphia, PA 19116

United States Sentencing Commission,
One Columbus Circle, NE., Suite 2-500,
Washington, DC 20002-8002,

Attention: Public Affairs.

- Should deceptive spammers get an "enhancement," i.e., a little more prison time, if they employ "sophisticated means" to send the spam?

YES

- Should the method the offender used to gather the targeted addresses be a consideration in sentencing? Under one proposal, spammers could face an enhancement for harvesting e-mail addresses from Web forums, or generating them randomly.

NO

- Should criminals who commit fraud, identify theft, child porn trafficking or other serious crimes be sentenced more severely if they sent unsolicited bulk e-mail in the course of the crime?

DEFINITELY!!!

January 20, 2004

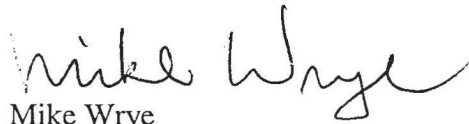
United States Sentencing Commission
One Columbus Circle, NE. Suite 2-500
Washington, DC 20002-8002

Attention: Public Affairs,

Subject: Spammer Sentencing Guidelines

Sentences for spamming should focus on high fines and little jail time. Take the profits out of spamming, but don't make the taxpayers support them during extended prison stays. Save the jails for violent people. Charge the spammers \$10 for each message they send and \$100 for each e-mail address they steal.

Thanks,

A handwritten signature in cursive script that reads "Mike Wrye". The signature is written in black ink and is positioned above the typed name and location.

Mike Wrye
Orlando, FL

United States Sentencing Commission
One Columbus Circle NE - Suite 2-500
Washington, DC 20002-8002

ATTN: Public Affairs

Recently, the following questions were posted in an article located at URL:
<http://www.securityfocus.com/news/7846> to which I have attached my responses which are formatted in two parts; a Yes/No response, followed by additional verbatim, expounding upon my position.

Q: Should deceptive spammers get an "enhancement," i.e., a little more prison time, if they employ "sophisticated means" to send the spam?

A: Yes.

Deception, in my opinion, not only includes using measures that conceal origin, but also those that hide content. The use of misspellings to evade content filters is becoming commonplace, and demonstrates that the sender already knows that the targets being emailed do not want to receive the message. An excellent example is the following misspellings of "Viagra" which include, but are not limited to, "Vigara," "Viarga," and "Vaigra." It should be mandated that **every individual advertisement or solicitation be prefixed with an ADV** as the first three characters of the subject, and that not using this identifier constitutes deception.

Q: Should the method the offender used to gather the targeted addresses be a consideration in sentencing? Under one proposal, spammers could face an enhancement for harvesting e-mail addresses from Web forums, or generating them randomly.

A: Yes

Harvesting techniques and randomly generated email addresses will automatically target people who do not want to receive any UCE.

Q: Should criminals who commit fraud, identify theft, child porn trafficking or other serious crimes be sentenced more severely if they sent unsolicited bulk e-mail in the course of the crime?

A: Yes

The UCE should always remain a separate offense. Sending child pornography and performing fraudulent activities should constitute an "offense enhancement" just as the use of deceptive headers and email address generation techniques.

In summary; **all unsolicited email should be double opt-in only**. This requires that an individual submit his email address to a particular marketer, then that marketer must send a confirmation to

that email address which must be answered. This will prevent unscrupulous persons from submitting the email addresses of other individuals, and will also prevent people who don't want to receive any email from having to opt-out from millions of possible emailing lists. In addition, all opt-in confirmations should have "OPT-IN?" as the first seven characters of the subject.

Spam is a **threat to national security** because of the bandwidth stolen (technological impact), the time wasted managing it (economic impact), and the aggravation it causes invokes a significant amount of collective bad will (health and possible criminal impact). Since national security is involved, spammers should be reclassified as saboteurs. This would also allow our military to reclassify spammers as "targets of opportunity" which makes those who reside overseas, legitimate military targets.

It is also important to distinguish that not only are the spammers guilty of criminal activity, but so are the businesses (and people) who employ them. The person who actually authorizes payment to a spammer should be held equally accountable for the crimes committed by the spammer because they are soliciting and financing the spammer's criminal activity.

It should also be required that ISPs give the option to their subscribers to be able to set up and upload IP and IP range blocks & country domain blocks. People who don't know anyone in China should be able to block the ".CN" domain without being forced to purchase special software.

In addition to prison time, spammers should be hit with draconian and mandatory minimum sentencing to include both prison time and financial penalties. Spammers maintaining American citizenship should be expatriated to a country from which they sent email. I propose a sentence of 1 year in prison and \$1,000 fine per each individual email recipient who did not authorize the marketer to solicit his business. For a spammer who sends a mere 100 UCEs to people who do not want to receive them, the spammer and the person who hired him should be sentenced to 100 years in prison and \$100,000 fine. The only way to terminate the spamming plague on society is to make examples.



TOM STATON

TOMSTAT@HOTMAIL.COM

2173 SANTA ANITA DR
LEXINGTON KY 40516



The safety and security association of the commercial explosives industry • Founded 1913

March 1, 2004

Via Hand-Delivery

United States Sentencing Commission
One Columbus Circle, NE., Suite 2-500
Washington, D.C. 20002-8002
Attention: Public Affairs

Re: Comments of the Institute of Makers of Explosives; U.S. Sentencing Commission; Sentencing Guidelines for U.S. Courts; Notice, 68 Fed. Reg. 75340 (Dec. 30, 2003). Issues for Comment 11: Hazardous Materials

Dear Sir or Madam:

IME is pleased to provide comments on the above-captioned Federal Register Notice.

IME is the safety association of the commercial explosives industry. Our mission is to promote safety and security and the protection of employees, users, the public and the environment; and to encourage the adoption of uniform rules and regulations in the manufacture, transportation, storage, handling, use and disposal of explosive materials used in blasting and other essential operations.

IME represents all U.S. manufacturers of high explosives and other companies that distribute explosives or provide other related services. Over 2.5 million metric tons of explosives are consumed annually in the United States of which IME member companies produce over 95 percent. These products are used in every state in the Union and are distributed worldwide. The value of these products is estimated to be in excess of \$1 billion annually. The ability to manufacture, transport, store, and use these products safely and securely is critical to this industry. Accordingly, IME is interested in any changes to the U.S. Sentencing Guidelines that have the potential to impact the transportation of hazardous materials.

We submit the following comments on the above-captioned notice.

(1) A New Guideline Should be Created to Address Offenses Involving HAZMAT Transportation

IME agrees in principle with the concern expressed by the U.S. Department of Justice (“DOJ”), that the current sentencing guideline applicable to hazardous materials (§2Q1.2 *Mishandling of Hazardous or Toxic Substances or Pesticides; Recordkeeping, Tampering, and Falsification; Unlawfully Transporting Hazardous Materials in Commerce*), is not adequately suited to hazardous materials (“HAZMAT”)-related transportation offenses.

As noted in the Federal Register notice, the §2Q1.2 Guidelines clearly are intended to cover offenses under the various U.S. environmental protection statutes and associated regulations and could, conceivably, be difficult to meaningfully apply to Department of Transportation (“DOT”)-regulated HAZMAT transportation offenses. For example, the only mention of transportation offenses in the §2Q1.2 Guidelines is at (b)(4); “If the offense involved transportation, treatment, storage, or disposal without a permit or in violation of a permit, increase by 4 levels.” §2Q1.2(b)(4). Clearly, this provision is directed at environmental *permitting* violations rather than the types of transportation-related offenses possible under DOT HAZMAT regulations. Where such offenses do not involve permitting, the Guideline is even less relevant as an appropriate tool.

Given the specificity of the current §2Q1.2 Guidelines to violations of environmental statutes, and the narrow, tailored structuring of the guideline to correspond to “typical” environmental recordkeeping and permitting requirements, and environmental “release” events, we believe there is substantial merit to DOJ’s recommendation that the §2Q1.2 Guidelines not be the sole frame of reference for sentencing violations of DOT HAZMAT requirements.

Accordingly, IME supports the alternative noted in the Federal Register Notice that a new guideline be created to more adequately and specifically address offenses involving the transportation of hazardous materials.

(2) An Appropriate Base Level For Offenses Involving the Transportation of Hazardous Materials Should Be Conservative Given the Diversity of Potential Hazards Posed by the Transportation of Commercial HAZMAT

As the Commission is no doubt aware, the transportation of hazardous materials is an essential, integral component of industrial and commercial activity and is ubiquitous throughout the United States (“U.S.”) and internationally. In addition, the quantity and variety of hazardous materials that are daily shipped in legitimate commerce in the U.S. is enormous, including widely recognizable materials such as gasoline to less obvious HAZMAT substances such as automotive airbags, various cosmetics, and a number of common food additives. Likewise, the relative potential danger – in a criminal context – posed by the myriad materials classified as HAZMAT varies as widely as the nature of the materials themselves.

While IME’s expertise in the area of HAZMAT transportation is limited to the transportation of explosives and related products, it is essential that the Commission fully appreciate the diversity and volume of these and other materials that are transported as HAZMAT. Similarly, the Commission should understand the potential (or lack thereof) that such materials might “provide a ‘target-rich’ environment for terrorists” or others with criminal intent. 68 Fed. Reg. at 75377. Any sentencing guidelines addressing hazardous materials offenses will necessarily and unavoidably have extraordinarily broad potential applicability and impact.



MARQUETTE
UNIVERSITY

March 11, 2004

United States Sentencing Commission
One Columbus Circle, NE
Suite 2-500
Washington, DC 20002-8002
Attn: Public Affairs

Re: Implementation of CAN-SPAM Act of 2003

Dear Sir/Madam:

We are responding to the request for comments regarding implementation of the CAN-SPAM Act of 2003 (69 Fed. Reg. 2169). We are law professors at Marquette University Law School.¹ Professor O'Hear teaches and writes in the field of federal sentencing. Professor Goldman teaches and writes in the field of Internet law.

We are troubled by the possibility that criminal spam violations might be referenced to the existing fraud guideline. In particular, we believe that spam violations² should not be sentenced by reference to the loss table for economic crimes. In the interests of just punishment and administrability, we instead urge the Commission to develop a new, simple, spam-specific guideline.

I. CAN-SPAM Violators Should Not Be Sentenced by Reference to the Fraud Guideline.

Fraud and other economic crimes are sentenced based principally on the amount of the loss intended or caused, according to the "loss table" set forth in U.S.S.G. § 2B1.1(b)(1). We have three principal concerns about tying CAN-SPAM violations to the loss table: (1) spam-caused losses are not appropriately analogized to losses from traditional economic crimes, (2) it would be difficult to accurately and fairly calculate spam-caused losses, and (3) loss table calculations would push most defendants towards the statutory maximum sentence, failing to adequately distinguish between defendants.

(1) Spam Violations Are Not Zero-Sum Crimes Like Economic Crimes.

A traditional economic crime is zero-sum: the defendant benefits at the direct expense of the victim. For example, in an embezzlement case, the defendant takes money from the victim

¹ The views expressed herein are our own and should not be attributed to Marquette University or Marquette University Law School.

² By "spam violations," we refer to criminal violations of new 18 U.S.C. § 1037.

for the defendant's benefit. Every penny gained by the defendant comes directly at the victim's expense. In contrast, spam violations are not zero-sum. In fact, the defendant may not gain anything, and the victim may not suffer a loss (or may even derive a benefit).

Specifically, § 1037(a)(2)-(5) criminalizes sending multiple commercial electronic mail messages ("MCEMM") using techniques that make it harder to find the sender or the email's source ("obscuring techniques"). However, a sender does not inherently derive any value from using obscuring techniques, nor is benefit to the sender an element of the crime. Likewise, obscuring techniques do not inherently deprive a victim of value. To be sure, obscuring techniques might frustrate efforts by recipients or Internet service providers to block the emails, but circumvention of blocking attempts is not an element of the crime, either.

Indeed, in some cases, some "victims" could benefit from MCEMM, irrespective of whether they were sent using obscuring techniques. For example, some service providers charge customers based on the volume of data they receive, in which case the service providers financially benefit from the higher volume. Moreover, some individual recipients find MCEMM helpful and valuable. Indeed, there would be no such thing as MCEMM if some percentage of recipients did not respond favorably to some of the email offers they receive.

Section 1037(a)(1) differs from the subsections criminalizing the use of obscuring techniques; the offense is instead premised on unauthorized use of a service provider's computer resources. Nevertheless, even this subsection does not require any sender benefit or victim detriment as an element of the crime. Even unauthorized use of resources does not necessarily cause harm if the service provider's computer had unused capacity at the time of the sender's campaign.

Thus, unlike traditional economic crimes, spam violations do not require a sender's gain at a victim's expense. No unwitting victim sends a check to the sender. No cash drawer comes up short. The victims may never know that they have suffered a "loss." Some "victims" may derive a benefit from the email. Thus, economic crimes predicated on a zero-sum calculus do not provide a proper analogy.

(2) Difficulty Computing Spam-Attributable Losses Will Lead to Considerable Administrative Costs.

We agree with Judge Jon O. Newman's general critique³ of the loss table: a table with sixteen different categories – and significant sentencing consequences in moving from one category to another – encourages considerable litigation over the meaning and measurement of "loss." This imposes needless burden on the court system. In theory, incremental loss should indeed produce incremental punishment, but the loss table carries this principle to an unwarranted extreme. In practice, the amount of loss shown at sentencing may depend on the diligence of the particular investigator working the case, random chance, and other variables having nothing to do with the defendant's actual culpability.

³ See Jon O. Newman, *Towards Guidelines Simplification*, 13 FED. SENT. R. 56 (2000).

The loss table's general weaknesses are magnified in the context of spam violations. As discussed above, injury (or even intent to injure) is not an intrinsic element of the offense. Thus, in some cases, spam violations may be truly victimless crimes.

Even where a colorable theory of loss can be advanced, connecting that loss to a particular sender's email may be difficult. Prosecutors and judges may be tempted to count as losses a service provider's "fixed costs," like a pro rata share of network operating costs, the amounts paid to third party vendors who attempt to block unwanted email, or the costs of employees on staff to remediate email campaigns. However, none of these costs are properly attributable to a particular defendant, as the service provider will incur these fixed costs no matter what any particular sender does.

It may be possible to link the sender's email with variable losses directly attributable to the email. Such losses might arise, for instance, if the defendant's email causes a service provider's network to go down, or requires a service provider's employees to work overtime to remediate a system problem. However, only a small percentage of email campaigns will cause these variable losses; hence, such losses may or may not be reasonably foreseeable to the defendant. In any event, collecting and presenting technical evidence of this nature will be a costly endeavor for prosecutors, victims and the court system.

Prosecutors and judges may also be tempted to consider an email recipient's lost time and annoyance, but these "harms" are not obviously cognizable under the fraud guidelines, which, by their own terms, are limited to "pecuniary losses." To be sure, a business victim might claim lost employee productivity from each individual recipient as a pecuniary loss, but determining such losses would create difficult assessments about the number of recipients who actually saw the email in their in-boxes and imprecise judgments about how much time was spent and how to cost-account for that time. Already, experts do not agree on how to calculate these economic costs,⁴ and some courts have rejected lost employee productivity entirely as a cognizable loss from spam.⁵

Meanwhile, under the loss table, defendants are entitled to a credit for the fair market value of property returned and services rendered to victims before the offense was detected.⁶ As discussed earlier, some recipients may find MCEMM valuable and take advantage of some of the offers they receive. Thus, so long as a defendant's email offered legitimate goods or services, the sentencing court might confront legally and factually complicated questions as to how to credit the defendant for goods and services provided to "victims."

Finally, courts might also confront difficult questions in determining how to apply the mass-marketing enhancement. The amount of the enhancement depends on the number of "victims."⁷ "Victim," in turn, is anyone who has suffered an "actual loss" for purposes of the

⁴ See, e.g., Saul Hansell, *Diverging Estimates of the Cost of Spam*, N.Y. TIMES, July 28, 2003, at C1.

⁵ See *Intel Corp. v. Hamidi*, 30 Cal. 4th 1342 (2003). The *Hamidi* case considered this issue in the context of a common law trespass to chattels claim.

⁶ USSG § 2B1.1, comment. (n.3(E)).

⁷ USSG § 2B1.1(b)(2).

loss table calculation.⁸ As the foregoing discussion illustrates, determining who suffers an actual loss from an MCEMM campaign will prove to be a difficult exercise.

In short, quantifying the loss in any individual case will likely prove contentious and costly. And – even after courts have resolved the chief legal questions in this area – in light of the idiosyncrasies of the loss definition and the difficulties of developing evidence of spam-related loss, the public will still lack any basis to conclude that sentences for spam violations actually distinguish between defendants based on the true gravity of their offenses.

(3) The Fraud Guideline May Lead to Unduly Severe Sentences for Spam Violations.

Spam violations are not necessarily serious criminal offenses. As noted above, § 1037 may be violated even by a sender promoting legitimate goods and services that some recipients actually want. While spam violations can involve culpable behavior (e.g., concealing the origin of an email campaign), the statute’s focus on improper marketing means – rather than improper marketing content or any unjust enrichment by the sender – places spam violations rather low on the culpability scale in comparison with the full range of socially undesirable behavior. Congress recognized the relatively benign nature of § 1037 violations by setting low maximum sentences of one and three years, depending on the violation.⁹

Yet, sentencing § 1037 violations pursuant to the fraud guideline would punish many defendants more seriously than is warranted by the crime’s nature. First, it is likely that spam defendants would routinely be subject to the sophisticated means enhancement.¹⁰ This sets a minimum offense level of twelve, which, for first-time offenders, would result in a sentence of 10-16 months. Putting this in a comparative perspective, even a low-volume sender whose messages caused no quantifiable injury would be subject to a mandatory penalty roughly equivalent to the penalty meted out to a person who embezzled \$30,000 or defrauded victims of a like amount. In our view, we should not equate spam violations with these more serious offenses.

Even if the Commission decided that the sophisticated means enhancement should not routinely apply to spam violators – and, at a minimum, we urge the Commission to do so – the fraud guideline might still treat many senders too harshly. Consider a low-volume defendant who sends one email to 500,000 recipients. A court considering lost employee productivity and a pro rata share of fixed costs might calculate the losses at \$0.10 per recipient,¹¹ for a total loss of \$50,000. In this case, the fraud guideline (including a six-level mass-marketing enhancement) would set the offense level at 18, requiring a minimum 27-month sentence for a first-time

⁸ USSG § 2B1.1, comment. (n.1).

⁹ A five-year maximum applies if the spam violation occurred in connection with another felony, or if the defendant has a relevant prior conviction.

¹⁰ USSG § 2B1.1(b)(8).

¹¹ Ferris Research published a cost analysis of spam concluding that employees receive 3.85 spam emails per day on average and that this volume costs employers \$9.90 per employee per month. *See Spam Control: Problems and Opportunities*, Ferris Research, Jan. 2003, at 16-17, available at <http://www.ferris.com/rep/200301/report.pdf>, Although the Ferris research report provides an illustrative data point for our critique, we do not endorse its methodology, and we suspect that it overstates losses substantially.

offender. Not only does this sentence seem high when compared to other offenses in a similar sentencing range (e.g., embezzlement of \$200,000), but it also comes close to the statutory maximum of three years. In other words, application of the fraud guideline may leave little room to distinguish between egregious and minor violators

Guidance to judges (through appropriate commentary in § 2B1.1) might help to avoid some of these problems, but, in some instances, in the interests of clarity and fairness, it is better to create a whole new guideline than to jerry-rig an old guideline for a new purpose. We believe that spam violations represent precisely such an instance.

II. The Commission Should Adopt a Simple New Guideline for CAN-SPAM Offenses.

As between the fraud guideline and the trespass guideline, we think the trespass guideline is the better analogy for spam violations for three reasons. First, many spam violations are analogous to common law trespass to chattels, because the onslaught of the sender's email can temporarily dispossess a victim of its "chattel" (i.e., the hardware used to operate a computer network).¹² Second, the trespass guideline excludes the problematic mass-marketing and sophisticated means enhancements. Third, the trespass base offense is lower, leaving more room to differentiate among defendants.

Unfortunately, the trespass guideline also incorporates by reference the fraud loss table for some offenses. Because no guideline referencing the loss table is an appropriate model for spam violations, we propose that spam violations be governed by a new spam-specific guideline.

Although the loss table taints the trespass guidelines, the closeness of the analogy makes the guidelines a useful starting point. Therefore, we propose a base offense level of four, identical to the base offense level for trespass. However, instead of using the fraud loss table, we propose increasing offense levels based on the aggregate number of recipients targeted by the sender in his or her MCEMM campaigns during the relevant time period.

This metric has three advantages. First, it is much simpler to calculate than loss. Indeed, the relevant evidence can be obtained directly from the defendant's records, potentially relieving victims of the burden of developing complex data for the government. Second, the amount of emails the sender tried to send is a reasonable proxy for victim harms. The more emails sent, the more likely it is that the sender caused some victims real harm at some point (e.g., by causing a recipient's server to crash). Third, the sender cannot foresee or prevent idiosyncratic victim losses, but the sender can control the number of recipients. Therefore, this metric will avoid sentencing discrepancies among senders who engaged in the same conduct, but who caused different degrees of "loss" as a result of chance (e.g., through sheer bad luck, one sent MCEMM to a network server at a time of unusual vulnerability, causing the server to go down).

To minimize litigation burdens, the spam guideline should include relatively few categories. For instance, the "volume table" might look like this:

¹² See Restatement (Second) of Torts, §§ 217-218 (1965).

| Number of Intended Recipients Of Illicit Email in a 12 Month Period¹³ | Increase in Level |
|---|--------------------------|
| 250,000 or less | no increase |
| More than 250,000 | add 3 |
| More than 1,000,000 | add 6 |
| More than 10,000,000 | add 9 |
| More than 100,000,000 | add 12 |
| More than 1,000,000,000 | add 15 |

We believe a base offense level of four plus this volume table adequately distinguishes egregious and minor violations.¹⁴ A sender targeting a billion recipients will receive the statutory maximum of three years, while a low-volume sender is treated more leniently.

Our proposal assumes simple § 1037 violations, i.e., the violations were not themselves conducted in furtherance of a scheme to defraud, distribute unlawful pornography, or commit any other crime. For aggravated spam violations, we believe that sentencing courts could and should take the linked offenses into account at sentencing as relevant conduct under the appropriate guidelines.

III. Conclusion

The guideline applicable to spam violations should be simple for courts to apply, but should also provide for meaningful distinctions among spam violators in at least rough proportion to the harm they have caused. We do not believe any guideline referencing the fraud loss table does that. Therefore, we believe that the Commission should develop a separate guideline for § 1037 violations that uses a volume table based on the number of intended recipients.

Respectfully submitted,



Professor Michael O'Hear
Assistant Professor of Law



Professor Eric Goldman
Assistant Professor of Law

¹³ A relevant time period should be defined for purposes of this table. We follow the statute's use, in a slightly different context, of an annual aggregation of MCEMM during the highest volume one-year period. See 18 U.S.C. § 1037(b)(2)(C).

¹⁴ There is, of course, nothing scientific about the cut-off points. They are intended to achieve meaningful differentiation at sentencing between the dabbler in spam, the professional, and the truly big-time player. The volume table is also intended to ensure that the full-range of statutorily available penalties (zero to three years in most cases) is, in fact, used, thus recognizing Congress's implicit belief that there are real differences in culpability among different spam violators. Wide ranges reduce the likelihood that a defendant will find himself or herself standing on (or falling off) a "cliff," i.e., just above or below a cut-off point. Still, there is admittedly some inevitable arbitrariness when cut-off points are defined. Thus, the fact that a given defendant's volume happens to be at the very top (or very bottom) of a range might, in conjunction with other factors, be made a basis for upward (or downward) departure in exceptional cases.

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=zdn>. 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 billion. 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 Health 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 simply 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 1, 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

Washington Legal Foundation
2009 Massachusetts Ave., N.W.
Washington, D.C. 20036
(202) 588-0302

March 15, 2004

United States Sentencing Commission
One Columbus Circle, N.E.
Suite 2-500
Washington, D.C. 20002
Attn: Public Affairs

Re: Comments on Proposed Amendment 2 to Sentencing Guidelines: Effective Compliance Programs in Chapter Eight. 68 Fed. Reg. 75340, 75354 (Dec. 30, 2003)

Dear Commissioners:

The Washington Legal Foundation (WLF) hereby submits these comments to the U.S. Sentencing Commission on Proposed Amendment 2 to the Sentencing Guidelines: Effective Compliance Programs in Chapter Eight. 68 Fed. Reg. 75354. In brief, WLF objects to the expansion of the definition of an effective compliance program for a business to include a program that detects and prevents *non-criminal* violations of laws and regulations. At the same time, WLF favors greater flexibility in the guidelines with respect to reducing an organization's culpability score. Finally, in response to the Commission's request for public comment on "any other aspect of the sentencing guidelines, policy statements, and commentary," *id.* at 75340, WLF reiterates its prior request to the Commission that it should review and amend its sentencing guidelines under Part 2Q with respect to environmental violations because of the unduly excessive prison sentences that have been meted out to first offenders for minor regulatory infractions.

Interests of WLF

WLF is a national non-profit public interest law and policy center based in Washington, D.C., with supporters nationwide. WLF has a longstanding interest in the work of the Sentencing Commission and the appropriate sentences that should be established for various categories of offenses.

Since the Commission's formation over 17 years ago, WLF has submitted written comments and has testified before the Commission on several occasions regarding various substantive issues. WLF has supported strict sentences for certain violent *malum in se* crimes, and more lenient sentences for others, particularly *malum prohibitum* violations, such as minor environmental regulatory infractions. For minor regulatory offenses, the underlying conduct is subject to myriad and often confusing rules and regulations, and would be better remedied by administrative and civil enforcement rather than by the heavy hand of criminal prosecution.

WLF has also litigated cases raising corporate criminal liability issues, particularly the growing and disturbing trend by the Justice Department to prosecute corporate employees and officers under the so-called "responsible corporate officer" doctrine that impermissibly allows the *mens rea* requirement to be diluted or ignored altogether. See *Hansen v. United States*, 262 F.3d 1217 (11th Cir. 2001), *cert. denied*, 535 U.S. 1111 (2002); *United States v. Weitzenhoff*, 35 F.3d 1275 (9th Cir. 1993), *cert. denied*,

513 U.S. 1128 (1995); *United States v. Ahmad*, 101 F.3d 386 (5th Cir. 1996); *United States v. Hanousek*, 176 F.3d 1116 (9th Cir. 1999), *cert. denied*, 528 U.S. 1102 (2000). WLF has also argued in court briefs and in communications to the Commission that prison sentences mandated by the guidelines for environmental offenses are draconian, arbitrary, flawed, and the result of double-counting the offense characteristics. Most recently, WLF represented three small U.S. seafood dealers, two of whom were each sentenced under the guidelines as first offenders to a draconian 97 months in prison for importing seafood in violation of the Lacey Act because the seafood was shipped in plastic bags instead of cardboard boxes. The Honduran seafood exporter also received a 97-month sentence. *See McNab v. United States*, 331 F.3d 1228 (11th Cir. 2003), *cert. denied*, 2004 U.S. LEXIS 1041; 72 U.S.L.W. 3535. *See also* Tony Mauro, "Lawyers Seeing Red Over Lobster Case," LEGAL TIMES (Feb. 16, 2004) (copy attached hereto).

WLF has also urged the Commission and its advisory committees to operate in a transparent manner when formulating Commission policy and guidelines with respect to corporate environmental offenses, and has taken the Commission to task and to court for failing to do so. *See Washington Legal Foundation v. U.S. Sentencing Comm'n*, 17 F.3d 1446 (D.C. Cir. 1993); *Washington Legal Foundation v. U.S. Sentencing Comm'n*, 89 F.3d 897 (D.C. Cir. 1996).

More pertinently, WLF submitted comments to the Advisory Group on Organizational Guidelines on May 20, 2002, outlining our general concerns about the organizational guidelines, and further noting our concerns that the Advisory Group did not include any in-house counsel or other corporate officer with first-hand experience with the operation of corporate compliance programs. Instead, the group consisted of primarily those professionals who, although knowledgeable of compliance programs, may have a different interest or perspective in evaluating such programs.

In addition, WLF's Legal Studies Division has published numerous studies, reports, and analyses on corporate criminal liability and related issues. *See, e.g.*, Joe D. Whitley, *et al.*, *The Case For Reevaluating DOJ Policies On Prosecuting White Collar Crime* (WLF Working Paper, May 2002); George J. Terwilliger, III, *Corporate Criminal Liability: A Handbook For Protection Against Statutory Violations* (WLF Monograph, 1998); William C. Hendricks, III and J. Sedwick Sollers, III, *Corporate Vicarious Criminal Liability* (WLF Contemporary Legal Note, April 1993); Alan Yuspeh, *Developing Compliance Programs Under The U.S. Corporate Sentencing Guidelines* (WLF Contemporary Legal Note, July 1992); Irvin B. Nathan and Arthur N. Levine, *Understanding And Complying With The U.S. Corporate Sentencing Guidelines* (Contemporary Legal Note, May 1992); Joseph R. Creighton, *New Corporate Sentencing Guidelines Are Vulnerable To Constitutional And Statutory Non-Compliance Challenges* (WLF Legal Backgrounder, March 6, 1992).

WLF Comments

1. Proposed Expansion of an Effective Compliance Program to Include "Violations of Law" Beyond Criminal Conduct.

Under Chapter 8 of the Sentencing Guidelines, the range of a fine that may be imposed on an

organization found guilty of a criminal offense is essentially computed by first determining the base fine, which generally involves a determination of the seriousness of the offense, and then multiplying the fine by the "Culpability Score" as determined under Section 8C2.5. The culpability score may be reduced by three points, under certain conditions, if the organization has an "Effective Program to Prevent and Detect Violations of Law." Section 8C2.5(f).

Heretofore, the Commission defined an "effective program to prevent and detect violations of law" in Application Note 3(k) to include seven characteristics, and defined "violations of law" to mean "criminal conduct." Application Notes 3(k) and 3(k)(1). Now, however, the Commission proposes to remove the definition of "effective compliance program" from its current location in the Application Notes and place it in a new stand-alone guideline. More troubling, however, the Commission proposes to broaden the definition of "violations of law" well beyond criminal conduct, and require that an effective compliance program be able to "prevent and detect" violations of any law, including civil and regulatory. In pertinent part, the Commission proposes to define "violations of law" to mean "violations of any law, whether criminal or noncriminal (including a regulation), for which the organization is, or would be, liable." Proposed Application Note 1 to Section 8B2.1.

WLF objects to this gross expansion of "violations of law" to include civil and regulatory offenses as unfair, unwarranted, and burdensome. If an organization were placed on probation, it would also involve the expenditure of scarce judicial resources to monitor an organization's compliance with non-criminal laws and regulations. Accordingly, WLF urges the Commission not to expand the definition of "violations of law" to include non-criminal conduct and offenses.

It has been estimated that there are over 300,000 federal regulations that subject a company to criminal liability, and that civil and administrative laws and regulations at both the federal and state level are countless. *See* Comments of the Association of Corporate Counsel at 3 (March 1, 2004). Civil and administrative violations do not involve criminal conduct and may occur inadvertently, despite the best compliance programs. Accordingly, organizations should not be penalized for failing to have a compliance program that, while otherwise effective in deterring and preventing criminal violations, is not designed to ferret out and prevent all manner of minor and trivial regulatory infractions. For example, under the proposed guideline, a company could be found not have an effective compliance program simply because there were inadvertent, minor, and non-harmful exceedences of emission or discharge limits under environmental regulations which would be comparable to driving a car 36 mph in a 35 mph zone. Indeed, an employee driving a company car in excess of the speed limit would disqualify the compliance program, as would other minor regulatory violations, such as allowing more persons in an office elevator or cafeteria than otherwise allowed by local building and safety codes.

The Commission has not articulated any reasons in the Federal Register as to why it believes that expanding the term "violation of law" to include federal, state, and local civil and administrative regulations is necessary. The report submitted by the Ad Hoc Advisory Group on Organizational Guidelines as well as the Commission's yearly sentencing statistics note that over 90 percent of the organizations sentenced under the guidelines had no compliance program at all. This suggests that the current compliance programs are working fairly effectively in detecting and preventing criminal conduct, and/or persuading the Justice Department not to file criminal charges in the first place if an offense occurred.

Indeed, WLF finds it remarkable and troubling that the Commission did not specifically solicit public comment as to whether it should greatly expand the definition of "violations of law" to include non-criminal regulations. Rather, the Commission seems to have already made up its mind on this issue, and is merely requesting comment as to whether the reduction in the culpability score for having an effective compliance program should be increased a paltry one point from the current three points to four points, "given the heightened requirements [*viz.*, expanding the definition of "violation of law" to include civil and regulatory offenses] for an effective program to prevent and detect violations of law under the proposed amendment." 68 Fed. Reg. 75360 (emphasis added). If it is a "given" that the Commission will expand the definition to include non-criminal provisions, the reduction in the score should be increased from the current three points to at least five points, rather than four.

Expanding the definition of violation of law to include civil and administrative regulations and provisions would simply be a costly "make work" requirement that would only benefit those who devise and implement compliance programs, or otherwise counsel companies on their compliance programs and the sentencing guidelines. Expanding the definition would skew priorities and drain corporate resources that could be better devoted to improving a compliance program to detect and prevent criminal activity, conduct which presumably is the most harmful to society. While the Advisory Group's desire is to foster a culture of compliance with respect to *all* federal and state regulations that are applicable to organizations, WLF believes that companies, rather than the Commission, can best decide how to devise compliance programs that are cost-effective and meaningful,

As we noted in our prior submission to the Advisory Group in May 2002, commentators have questioned this "feel good" approach to developing sentencing policy.

One of the continuing debates about criminal punishment concerns the extent to which the precise determination of penalties within the criminal sentencing process effectively serves any utilitarian goal of public law enforcement or is merely political theater. Even if we grant the point that some criminal sanction is more useful than none, there remain the questions of whether and when it is worthwhile at the margin to devote resources to refinements in the formal criminal penalty determination system, except perhaps as required to preserve marginal deterrence.

Jeffrey S. Parker & Raymond A. Atkins, *Did the Corporate Criminal Sentencing Guidelines Matter? Some Preliminary Empirical Observations*, 42 J. Law & Econ. 423, 424 (Apr. 1999). The Commission should keep in mind as it develops and amend the guidelines that while punishment and deterrence are indeed the goals of sentencing, Congress mandated that punishment and fines that are imposed by courts should be "sufficient, *but not greater than necessary*" to comply with the purposes of punishment and deterrence. 28 U.S.C. § 3553(a) (emphasis added). Accordingly, the Commission's and the Advisory Group's rejection of optimal penalties policy, and the lack of empirical evidence to determine what punishments have been effective without causing overdeterrence or gratuitous punishment, runs counter to Congress's express policy of conservation of punishment.

2. Eliminating the Prohibition on Three-Point Reduction for Delaying Reporting of Offense.

The Commission also requested public comment as to whether the current prohibition on the receipt of a three-point reduction under Section 8C2.5 for unreasonably delaying reporting an offense to

the proper authorities should be modified so that the organization could at least be considered for a reduction. 68 Fed. Reg. 75359. WLF agrees with this flexible approach that the organization should be considered for a reduction, and that the current rule should be eliminated. What some may regard as an unreasonable delay, may in fact be legitimate due to the company's desire to investigate the incident thoroughly to determine whether a violation has in fact occurred and the extent of the alleged violation.

3. Changing Automatic Preclusion under Section 8C2.5(f) To a Rebuttal Presumption.

The Commission also requests comment as to whether Subsection (f) of Section 8C2.5 should be amended as proposed to change the automatic preclusion of a three-point reduction if certain high-level individuals participated in, condoned, or were wilfully ignorant of the corporate offense, to one where there is a rebuttable presumption that the three-point reduction does not apply. 68 Fed. Reg. 75359. WLF supports this more flexible approach and believes that the corporation should be able to show on a case-by-case basis why it believes that its compliance program deserves a reduction. Accordingly, the automatic preclusion should be changed to a rebuttable presumption of preclusion.

4. Other Areas of Sentencing Policy That Should Be Addressed.

Finally, the Commission requests comment on any other areas of sentencing policy that should be addressed. WLF has requested the Commission on several occasions that it should review the application of prison sentences meted out for violations of environmental offenses under Part 2Q. Criminal enforcement of environmental laws of both individuals and corporations have been growing over the years, and raise serious issues both respect to penalties for corporations, as well as those imposed on individuals in the form of lengthy and unwarranted prison terms under Sections 2Q1.2 and 2Q1.3 of the guidelines. In many cases, the Department of Justice overcharges by adding money laundering and other charges to the underlying substantive environmental offenses in order to drive up the sentencing score, resulting in grossly excessive sentences for what otherwise would be minor regulatory offenses.

As noted, a federal judge was forced to impose a draconian 97-month sentence on first offenders, which was at the low end of the 97-127 month range as determined by the guidelines, for the "crime" of importing seafood in plastic bags instead of cardboard boxes under the Lacey Act. *See McNab v. United States*, 331 F.3d 1228 (11th Cir. 2003), *cert. denied*, 2004 U.S. LEXIS 1041; 72 U.S.L.W. 3535. This prison sentence, longer than that meted out to some drug dealers, is, by any reasonable person's standards, clearly "*greater than necessary*" to comply with the purposes of punishment and deterrence under 28 U.S.C. § 3553(a). There are many other examples of unjust and excessive prison sentences that have been and are being imposed under the guidelines which call out for serious reconsideration and revision by this Commission. At a minimum, the Commission should have its staff or an advisory group review this problem area.

Conclusion

WLF appreciates the opportunity to provide these comments and urges the Commission to carefully consider the full impact that its guidelines and the proposed amendments would have on organizations before proposing them to Congress.

U.S. Sentencing Commission
March 15, 2004
Page 6

Respectfully submitted,

Daniel J. Popeo
General Counsel

Paul D. Kamenar
Senior Executive Counsel

encl

Select '**Print**' in your browser menu to print this document.

©2004 Legal Times Online

Page printed from: <http://www.legaltimes.com>

[Back to Article](#)

Lawyers Seeing Red Over Lobster Case

Tony Mauro
Legal Times
02-16-2004

A dispute that began with a shipment of Honduran lobsters into Alabama has turned into an international incident that is now before the Supreme Court, complete with high-powered law firm and interest group participation.

At its Feb. 20 private conference, the Court will consider whether to add *McNab v. United States*, No. 03-622, and *Blandford v. United States*, No. 03-627, to its docket. The cases raise delicate issues of federal court interpretation of foreign law at a time when the Supreme Court itself is taking a fresh look at the importance of international law in its own jurisprudence.

Honduran citizen David McNab, a lobster fleet owner, and Robert Blandford and two other American seafood importers were arrested in Alabama in 1999 for importing 70,000 pounds of Caribbean spiny lobsters, a few of which were undersized and all of which were in plastic bags — in violation of a Honduran regulation that required shipment in cardboard boxes.

The four were indicted in federal court in Alabama for violations stemming from the Lacey Act, which prohibits the import of fish or wildlife taken or sold in violation of U.S. or "any foreign law." The fact that the shipment violated Honduran regulations was the predicate for a range of criminal charges, including money laundering. McNab, Blandford, and a third defendant were convicted and sentenced to eight years in prison. The fourth was sentenced to two years.

Meanwhile, as part of their legal battle, the importers successfully challenged the validity of the regulations in Honduras.

On appeal in the U.S. courts, the lobstermen claimed that the change in Honduran law dictated reversal of their U.S. convictions. The government of Honduras filed a brief in the appeal, asserting that the laws had no force at the time of the arrest, but the U.S. Court of Appeals for the 11th Circuit affirmed the convictions by a 2-1 vote.

The 11th Circuit acknowledged that a nation's own officials are "among the most logical sources" for interpreting that nation's laws. But the court concluded that, when a foreign government changes its position about those laws, the United States is not bound by the new interpretation. Heeding the new interpretation, the 11th Circuit majority stated, would lead to the "endless task of redetermining foreign law."

The 11th Circuit also suggested that future defendants with "means and connections" in a foreign country could lobby that country's officials to invalidate their laws as a way of undermining U.S. prosecutions. Circuit Judge Charles Wilson wrote the opinion,

joined by Judge Frank Hull.

In dissent, Senior Judge Peter Fay said the current Honduran interpretation should prevail, adding that the process of legal change criticized by the majority "occurs routinely in our country."

Former D.C. Circuit nominee Miguel Estrada, a Honduran native who is a D.C. partner at Gibson, Dunn & Crutcher, represents McNab in his appeal to the Supreme Court. "The 11th Circuit is alone among the courts of appeals in refusing to accord deference to the construction of foreign law adopted by the authorized representatives of the foreign states," Estrada tells the Court.

Former Solicitor General Seth Waxman, now a D.C. partner at Wilmer, Cutler & Pickering, filed a brief in the case for the Honduran government. "Mr. McNab's actions did not violate any valid or enforceable law in Honduras," Waxman says in the brief, also noting that Honduras "desires to protect its citizens from misapplication of Honduran law."

The lengthy prison term for seemingly minor trade violations, as well as the appeals court's decision to not follow Honduran legal authority, has given the case high visibility in Honduras. And it has been framed in the United States as an international criminal law equivalent of the McDonald's too-hot coffee cup — an example of laws and punishment run amok.

"It's a classic case of over-criminalization — honest people being sent to prison for eight years for using plastic instead of cardboard," says Paul Kamenar, senior counsel at the Washington Legal Foundation, which filed the petition on behalf of Blandford.

An unusual coalition of groups — including the National Association of Criminal Defense Lawyers and the National Association of Manufacturers — also filed a brief, bemoaning the increasing use of criminal law to enforce economic regulations when no criminal intent is shown.

In a brief by Paul Rosenzweig, a lawyer at the Heritage Foundation, the groups tell the Supreme Court that the elimination of criminal intent requirements "allows the government to engage in grotesque over-charging such as that demonstrated here — pyramiding trivial civil infractions of uncertain (and now disavowed) foreign law into smuggling and money laundering offenses that carry astronomical and unjust domestic criminal penalties."

The Justice Department defends the conviction before the high court.

"If the laws were valid in Honduras during the time period covered by the indictment, the defendants violated the Lacey Act," the government's brief states. "Whatever changes in the laws occurred after the lobsters were imported into the United States illegally have no effect on the defendants' convictions."

Deputy Solicitor General Paul Clement signed the brief, which notes that Solicitor General Theodore Olson is recused in the McNab case. Before becoming solicitor general in 2001, Olson was a partner at Gibson, Dunn, the firm that represents McNab.



March 15, 2004

United States Sentencing Commission
One Columbus Circle, N.E., Suite 2-500,
Washington, D.C. 20002-8002
Attention: Public Affairs

Re: Comments in Proceeding BAC2210-40/2211-01

Dear Mr. Courlander:

The Internet Commerce Coalition appreciates the chance to respond to the Sentencing Commission's request for comments regarding the guidelines that will apply to criminal spam sent in violation of 18 U.S.C. § 1037. The Internet Commerce Coalition's ("ICC's") members include major ISPs and e-commerce companies and associations: AT&T, BellSouth, Comcast, eBay, MCI, SBC, TimeWarner/AOL, and Verizon, the U.S. Telecomm Association, CompTel and the Information Technology Association of America.

Curbing and deterring spam is a major priority for the ICC and its members. The ICC worked actively to support passage of § 1307 as part of the CAN-SPAM Act, and provided extensive factual and technical information to the authors of this part of the legislation. Section 1037 prohibits the major falsification and hacking methods that professional spammers use to evade software that protects users and ISP networks from spam.

I. OVERVIEW OF THE SPAM PROBLEM

Spam currently constitutes over half of all traffic on the Internet. It floods user inboxes, and burdens ISP and corporate networks. The economic costs of spam have been estimated to be nearly \$9 billion in 2002, according to a study by Ferris Research. Spam is also the leading complaint of Internet users regarding their Internet experience.

Most spam is sent in violation of federal and state fair trade practice laws, and civil spam laws. ICC members have sued well over 100 spammers, and the FTC has brought a large number of enforcement actions against spammers. These efforts have thus far not dissuaded professional spammers, who routinely employ falsification and hacking methods prohibited by from continuing to increase the volume of spam on the Internet. Many of the largest spammers continue to live in the United States sending out hundreds of millions of spam emails using these methods with relative impunity. Indeed, 8 of the top 10 spammers worldwide as measured by the anti-spam organization Spamhaus live in the United States. See <http://www.spamhaus.org>. Foreign governments and ISPs routinely complain about the huge volume of spam that comes from the U.S.

For these reasons, ICC members are convinced that criminal enforcement against professional spammers who rely on the hacking and falsification tactics prohibited by § 1037 is essential to reduce the spam problem. Large-scale professional falsification spammers and their co-conspirators are willing to risk the threat of civil litigation. However, if they perceive that continued violations create a meaningful risk of prosecution and significant prison time (not probation), we believe that U.S. spammers will find a different line of work, and the rising tide of spam will abate.

Section 1037 prohibits knowingly “initiating” illegal messages, and defines “initiate” as including both transmitting and procuring the transmission of the illegal emails. 15 U.S.C. § 7702(9). Spammers who use falsification tactics prohibited in § 1037 and the advertisers who knowingly procure and profit from their activities are fundamentally different from legitimate companies who use email for promotional purposes. These spammers and businesses who rely on spam regularly employ highly fraudulent and deceptive conduct such as computer hacking, wire and mail fraud, false and deceptive advertising, and misappropriating the identities of others in order to obtain computers, email accounts, Internet domains or Internet protocol addresses from which to spam, use of multiple bank accounts and use of sham corporations. These egregious activities are very similar to those of other criminal enterprises that are treated severely under the Sentencing Guidelines. They are also fundamentally different from the ways that legitimate businesses and individuals use email, so that there is little risk of the prohibitions in § 1037 being applied unjustly.

The worst of the advertisers who advertise by means of these outlawed techniques have a policy or practice of paying others to advertise their products and services in ways that violate § 1037. The entities often compensate spammers who send email on their behalf by paying for sales leads or by paying commission on actual sales. In addition to the knowledge of the illegal conduct, factors to consider in sentencing such individuals or corporations include whether the conduct appears to be grounded in either written or unwritten policy or established practice; whether there is evidence of similar conduct in a significant proportion of the defendant’s email campaigns; and whether the procurer had the ability to control the illegal spamming activity.

Because of the significant harm caused by and egregious tactics used by professional violators of § 1037, and the need for sufficient incentives for criminal prosecution of spammers, the ICC urges the Commission to set sufficiently strong penalties for violations of this statute.

II. ANSWERS TO THE COMMISSION’S QUESTIONS

(1) What are the appropriate guideline penalties for a defendant convicted under 18 U.S.C. § 1037?

(a) Should the new offense(s) be referenced in Appendix A (Statutory Index) to §§ 2B1.1 (Fraud, Theft, and Property Destruction), and 2B2.3 (Trespass), and/or to some other guideline(s)?

It is our view that § 1037 offenses are properly referenced in Appendix A to § 2B1.1, the fraud, theft, and property destruction guideline. Spammer falsification and hacking tactics are most closely related to conduct covered in this guideline, and particularly to the penalty offense levels provided for computer hacking set forth in § 2B1.1(b)(13) that were implemented after the passage of the Homeland Security Act. On the other hand, the penalties for the more serious § 1037 offenses, including those involving highly organized sophisticated business operations and massive volumes, may deserve more severe penalties than those available for many of the hacking offenses. At the same time, some of the violations may be minor in nature. As a result, the guidelines provisions should not be so inflexible as to prevent probation sentences in some instances.

The trespass guideline, § 2B2.3, is far less suitable since the offense levels within this guideline are low and do not properly reflect the seriousness of § 1037 violations. There certainly may be situations where § 1037 offenses may be linked to offenses involving sexual exploitation of minors and obscenity (§§ 2G1.1, 2G1.2 and 2G1.3) and offenses involving criminal enterprises and racketeering (§ 2E1.1).

(b) What is the appropriate base offense level for the new offense(s)?

We believe that the base offense level of 6, which is used for § 2B1.1, would be an appropriate starting point for § 1037 offenses. This is particularly the case as just noted because there will be minor offenses that would properly be dealt with by probationary sentences.

(c) Should the offense level vary depending on the seriousness of the offense (for example, should the base offense level for a regulatory violation under 18 U.S.C. § 1037 be the same as the base offense level for a more serious violation under that statute)?

The statute makes it clear that offense levels should vary depending upon the seriousness of the offense and provides the Commission with clear directions in this regard. We take no position with reference to regulatory violations.

(d) If 18 U.S.C. § 1037 is referenced to § 2B1.1, should special offense characteristics be added to that guideline that ensures application of the multiple victim enhancement at § 2B1.1(b)(2)(A)(I) or the mass marketing enhancement at § 2B1.1(b)(2)(A)(ii) to a defendant convicted of 18 U.S.C. § 1037? Should a defendant convicted under 18 U.S.C. § 1037 receive an enhancement under § 2B1.1(b)(2)(A)(i) or (ii) based on a threshold quantity of email messages involved in the offense, and if so, what is that threshold quantity? Another option which might be better is to create special offense characteristics for § 1037 offenses.

We strongly recommend that special offense characteristics be used to enhance sentences for more serious and sophisticated violations of § 1037. First of all, the statute reflects Congress' intent that a threshold quantity of email messages – 2,500 per day, 25,000 per month or 250,000 per year – should be taken into account in determining enhancement of the defendant's sentence.

In order for Internet Service Providers to protect their network and subscribers, they have developed sophisticated techniques to eliminate spam messages before they get into the service.

Spammers typically destroy as much of the technical trail of their spamming as possible in order to avoid detection. Additionally, most ISPs along the trail through which a spam message travels typically do not preserve the relevant transmission logs for an extended period, due to the massive volumes of data involved in keeping track of the communications that cross their networks every day. Some companies (like AOL) may be able to provide evidence of the violation only by obtaining and storing consumer complaints, which have proven to be only a small fraction of the volume of email that a professional spammer actually transmitted or attempted to transmit. In AOL's experience, the volume of email actually sent by a spammer is several orders of magnitude larger than the volume of complaints received about that spammer. Recognizing these factors, Congress set the appropriate felony trigger for volume at 2,500 per day/25,000 per month and 250,000 per year. Proof of a continuing pattern of violations above this level should trigger an enhancement of the sentence beyond the baseline felony level.

Section 1037(a) and (b)(2) offenses should include at least the following special offense characteristics:

1. Increases to the base offense level for each of the factors listed in the statute: offense committed in furtherance of felonies; prior convictions; use of false account or domain name registrations; message volume; proof of victim loss or offender gain, including injuries to consumers caused by loss of access to accounts or equipment or because of identity theft; and major leadership role in the offense;
2. Increases to the base offense level for the use of sophisticated means; and
3. The addition of language to § 2B1.1(b)(8) (the provision which increases the offense level for relocating operations to evade law enforcement) to include specific language addressing evasion techniques spammers use to evade detection.

The sophisticated means enhancement should include using methods that evade secure email systems under development that authenticate senders or Internet domains used by a senders as legitimate by means of digital certificates. If a defendant cracks the security of a sender authentication technology or shares that information with others, or steals the identity of a trusted sender of email in order to send spam, an enhancement of at least 2 levels is warranted, and similar to the provisions of § 2B1.1(b)(9), if the resulting offense level is less than level 12, there should be an increase to that level.

(e) Under what circumstances shall an offense under 18 U.S.C. § 1037 be considered to involve sophisticated means?

As just noted, in light of the serious problems created by "professional spammer" falsification tactics, use of sophisticated means should trigger an enhancement. Section 1037(b) sets out a series of factors that reflect sophisticated means for committing the offense and that merit an enhancement for sophisticated means. These include sending a high volume of email and supervising others in the offense. Presence of these factors might trigger an enhancement to level 14 (15-21 months).

In addition, several other factors not specified in the statute reflect efforts to conceal the offense and would merit enhancements that might be similar to § 2B1.1(b)(8) of the Guidelines. These include:

- (a) destruction of email records by a spammer;
- (b) use of computer facilities outside the boundaries of the United States, a common method by which sophisticated spammers attempt to evade enforcement in the U.S.; and
- (c) use of shell corporations or multiple bank accounts to evade detection.

Each of these factors are sufficiently serious to warrant enhancements of 2 levels.

(f) Consistent with the directive in section 4(b)(2) of the CAN-SPAM Act of 2003, should § 2B1.1 contain an enhancement for defendants convicted under 18 U.S.C. § 1037 who (I) obtain e-mail addresses through improper means, including the harvesting of e-mail addresses from the users of a website, proprietary service, or other online public forum without authorization and the random generating of e-mail addresses by computer; or (ii) knew that the commercial e-mail messages involved in the offense contained or advertised an internet domain for which the registrant of the domain had provided false registration information?

In our view, each of these factors also should trigger enhancements.

1. Harvesting email addresses by automated means, in violation of the rules of the online service or online forum where those addresses are posted, is a significant source of unwanted spam that penalizes the use of public fora such as personal or professional web pages, online marketplaces and Internet discussion fora. It chills free speech on the Internet and chills e-commerce in public fora.

2. Dictionary attacks occur through several ways. The first is a “phone book attack,” in which a spammer generates email addresses corresponding to all possible name and first initial combinations in the phone book of one or more large metropolitan areas. The second is a pure random alphanumeric attack—the spammer sends to every alphanumeric combination permitted, for example, in a 16 character AOL address prefix. The third method is sending email to “culled” lists originally generated using any of the two previous techniques, but where the spammer has run the list once and culled out the invalid addresses based on records of undeliverable emails. Dictionary attacks are in effective methods used to obtain a password to which to send spam and thereby to access target accounts for illicit purposes. Such attacks generate a very large number of emails sent to false addresses and significantly burden networks with returned emails. Given the seriousness of dictionary attacks, enhancements should be increases of up to 6 levels, comparable to § 2B1.1(b)13(A)(iii) offenses.

3. Advertising or including an Internet domain with false registration information is a common tool by which the spam kingpins who pay for spam to be sent out on their behalf evade detection. Use of any of these means might result in an increase of 5 offense levels.

(g) Which adjustments should be considered directly pertinent to § 1037 offenses?

There are adjustments in Chapter 3 that could be pertinent to § 1037 offenses. These include the vulnerable victim adjustment under § 3A1.1; the role in the offense aggravating and mitigating adjustments under §§ 3B1.1 and 3B1.2; the abuse of trust or use of special skill adjustment under § 3B1.3; and the obstruction or impeding the administration of justice adjustment under § 3C1.1. Unless they are utilized as special offense characteristics in § 2B1.1, these adjustments should be used to significantly increase offense levels (and, in the case of an individual with a minor role in the offense, or a minor duped into spamming activity by a sophisticated spammer, to decrease the levels). In order to ensure that the factors are used in calculating penalties, it might be preferable to incorporate these adjustments as special offense characteristics.

The vulnerable victim adjustment should apply, for example, where spammers impersonate an innocent person in the course of the violation—e.g., by hacking into another person's account and sending spam, falsely placing that person's email address in the "from" line of spam emails, or using another person's identification information in registering for an email account, domain name or to obtain their Internet Protocol address space. Such tactics smear another person's name, can cause that other person to lose good will or to lose access to the Internet, and even to receive death threats from outraged recipients of offensive spam.

(2) What are the appropriate guideline penalties for offenses other than 18 U.S.C. § 1037 (such as those specified by section 4(b)(2) of the CAN-SPAM Act of 2003, i.e., offenses involving fraud, identity theft, obscenity, child pornography, and the sexual exploitation of children) that may be facilitated by the sending of a large volume of unsolicited e-mail?

Specifically, should the Commission consider providing an additional enhancement for the sending of a large volume of unsolicited email in any of the following: § 2B1.1 (covering fraud generally and identity theft), the guidelines in Chapter Two, Part G, Subpart 2, covering child pornography and the sexual exploitation of children, and the guidelines in Chapter Two, Part G, Subpart 3, covering obscenity? Alternatively, should the Commission amend existing enhancements, or the commentary pertaining thereto, in any of these guidelines to ensure application of those enhancements for the sending of a large volume of unsolicited email? For example, should the Commission amend the enhancements, or the commentary pertaining to the enhancements, for the use of a computer in the child pornography guidelines, §§ 2G2.1, 2G2.2, and 2G2.4, to ensure that those enhancements apply to the sending of a large volume of unsolicited email?

As reflected earlier, violations of § 1037 that involve violations of other serious felony statutes should trigger an enhancement of the § 1037 that makes the offense level comparable to what it would have been if the sentencing guidelines for the other provisions would have been used.