

In addition to the insertion of the term "oxycodone" into Application Note 9, for purposes of consistency, the term "oxycodone (actual)" should also be added to Note B of the Drug Quantity Table after "Methamphetamine (actual)". The term oxycodone should not, however, be added after "metamphetamine" in the second sentence. This portion of the note currently indicates that for those narcotics which have guidelines based upon both narcotic mixture and actual narcotic weight, in the case of an offense involving a mixture containing the narcotic, the greater of the offense levels determined by the weight of the mixture and the weight of the actual narcotic should be used. This inclusion would negate the intended impact of the proposed amendments for offenses involving Percocet branded oxycodone, but for the striking of the phrase "1 gm of Oxycodone = 500 gm of marihuana" in the Drug Equivalency Tables.

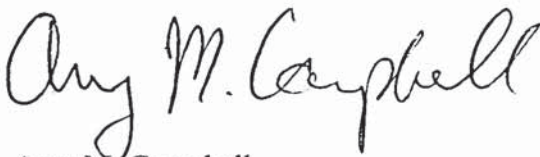
The third issue I would like to address concerns the striking of "1 gram Oxycodone=500 grams marihuana" and the insertion in its place of "1 gram Oxycodone (actual)=6700 grams marihuana." As discussed above, I readily agree that the appropriate measure of the narcotic oxycodone (and indeed, all narcotics) for sentencing purposes should be the actual weight of the narcotic itself, and not the weight of the pill or capsule containing the narcotic; and further, that leaving in the original equivalency would subject oxycodone offenses to the "greater of" standard in Note B discussed above, which in turn would negate the intended effect on Percocet offenses. However, the proposed equivalency of one gram Oxycodone (actual) to 6700 grams (6.7 kilograms) marihuana seems rather arbitrary. The proposed new equivalency appears to be based on the translation of the current equivalency using the actual oxycodon percentage by weight in 10-milligram dosages of Oxycontin branded oxycodone tablets. While this new equivalency clearly serves the stated purpose of substantially reducing penalties for trafficking in Percocet, the notice of proposed amendments provides no indication of the criteria considered in

establishing this proposed equivalency. A review of such criteria would be helpful in assessing the appropriateness of the proposed equivalency, particularly since other opiate equivalencies are based upon mixture weights rather than actual weights.

The fourth issue I would like to address is the retroactive application of the proposed amended guidelines. Previously, any offense involving less than 10 grams of oxycodone (mixture) was subject to the level 12 sentencing floor, and under the proposed amendments would continue to be subject to such floor for offenses involving less than 10 grams Oxycodone (actual). Thus, individuals receiving sentences for such offenses would not be able to avail themselves of §1B1.10 (Reduction in Term of Imprisonment as a Result of Amended Guideline Range). However, any offense previously involving more than 10 grams of Oxycodone (mixture) would result in a lower sentence under the proposed amendments, and thus the proposed amendments should be made retroactive to previously sentenced defendants.

I appreciate your consideration of these comments.

Sincerely,



Amy M. Campbell

Palliative Care Fact Sheet

No. 2 November 2002

A Monthly Service to General Practitioners in the Hunter Region

Director: Prof P Ravenscroft
 Phone: (02) 49211954
 Fax: (02) 49211952
 Editor: Dr John Cavenagh

Information in this Fact Sheet does not necessarily represent the views of the editor or the editor's advisers. The editor and the editor's advisers are not liable for any damages or claims by third parties arising from this material.

Palliative Care is the care and study of Patients with active, progressive, far advanced disease, where the prognosis is limited and where quality of life issues are the central concern. The care also involves families / carers. The patient's GP is a key member of the Palliative Care team.

Pain & Symptom Management - Opioid Conversion Table

This conversion chart has been compiled from a number of sources but the most heavily relied on source is the Therapeutic Guidelines series on Analgesics and Palliative Care editions. Other important resources for opioid conversions are the Australian Medicines Handbook 2001 Edition, and the excellent website called Palliative Drugs <http://www.palliativedrugs.com.au>

CONVERSION EXAMPLES:

1. CONVERT from Oral MORPHINE to S/C MORPHINE	RATIO
Oral Morphine 30mg 4 th hrly = S/C Morphine 10mg 4 th hrly	3 : 1
2. CONVERT from Oral MORPHINE to ORAL OXYCODONE (ENDONE)	RATIO
Oral Morphine 30mg 4 th hrly = Oral Oxycodone (Endone) 30mg 4 th hrly	1 : 1
3. CONVERT from Oral MORPHINE to ORAL HYDROMORPHONE	RATIO
Oral Morphine 30mg 4 th hrly = Oral Hydromorphone 4mg 4 th hrly	7.5 : 1
4. CONVERT from Oral MORPHINE to S/C HYDROMORPHONE	RATIO
Oral Morphine 30mg 4 th hrly = S/C Hydromorphone 1.5mg 4 th hrly	20 : 1
5. CONVERT from Oral MORPHINE to Oral METHADONE (SEEK ADVICE)	
1 If the morphine dose is less than 300mg/day: Oral Morphine 30mg 4 th hrly (180 mg/day) = Oral Methadone 10mg bd (20 mg/day) 2 If the morphine is greater than 300mg/day: Start at 30mg/d and titrate according to response, it may take over a week to get to steady-state concentrations. It is strongly recommended to liaise with Pain or Palliative Care staff. Due to incomplete cross tolerance and its long half-life ~10 : 1 inpatient admission is recommended for this conversion to ensure close observation of the patient.	
6. CONVERT from Oral CR MORPHINE to Oral CR OXYCODONE	RATIO
CR Morphine 30mg bd (MS Contin 30mg bd or Kapanol or MSMono (60mg ONCE daily)	= CR Oxycodone (Oxycontin) 20mg bd 1.5 : 1

Exhibit A

[98]

7. CONVERT from ORAL CR MORPHINE to CR OXYCODONE		RATIO
Oral CR Morphine 60mg/d (MS Contin 30 mg bd or Kapanol or MSMono (60 mg ONCE daily))	= CR Oxycodone (Oxycontin) 20mg bd	1.5 : 1
8. CONVERT from CR MORPHINE to S/C MORPHINE		RATIO
Oral Morphine 30mg bd (60 mg/d)	= Morphine 20mg CSCI / 24hrs	3 : 1
9. CONVERT from S/C MORPHINE to S/C FENTANYL		RATIO
Morphine 10mg	= Fentanyl 150i grms	70 : 1
10. CONVERT from S/C MORPHINE to S/C SUFENTANIL		RATIO
Morphine 300mg/24hrs CSCI	= Sufentanil 450i grms CSCI / 24hrs	700 : 1
11. CONVERT from CSCI MORPHINE to INTRATHECAL MORPHINE		RATIO
Morphine 100mg CSCI / 24hrs	= Morphine 1mg IT daily	100 : 1
12. CONVERT from S/C MORPHINE to EPIDURAL MORPHINE		RATIO
Morphine 100mg CSCI / 24hrs	= Morphine 10mg E / 24 hrs	10:1
13. CONVERT from S/C MORPHINE to Intraventricular MORPHINE		RATIO
Morphine 100mg CSCI / 24hrs	= Morphine Intraventricular 0.1mg / d	1000 : 1
14. CONVERT from S/C FENTANYL to Transdermal FENTANYL		RATIO
Fentanyl 600i grms / 24 hrs via a continuous s/c infusion	= Transdermal Fentanyl 25i grm/hr	1 : 1
15. CONVERT from S/C FENTANYL to Sublingual FENTANYL		RATIO
Fentanyl 50i grms	= Fentanyl 50i grms	1 : 1
16. CONVERT from S/C FENTANYL to S/C SUFENTANIL		RATIO
Fentanyl 100µgrm	= Sufentanil 10µgrm	10:1

ABBREVIATIONS

CR = Controlled Release
 S/C = Subcutaneous
 IT = Intrathecal
 CSCI = Continuous subcutaneous Infusion
 S/L = Sublingual
 E = Epidural

• The conversions contained in this Fact Sheet are average equivalents because of pharmacokinetic variation from patient to patient. If in any doubt contact Palliative Care. Editor



Crown Quadrangle
559 Nathan Abbott Way
Stanford, CA 94305-8610

Tel: 650.723.5674
Fax: 650.723.4426

March 17, 2003

Via Overnight Mail

Office of Public Affairs
United States Sentencing Commission
Attn: Karen Hickey
One Columbus Circle, N.E.
Washington, D.C. 20002-8002

Re: Comments re Section 1030 Guidelines

Dear Ms. Hickey:

On behalf of Commentators **National Association of Criminal Defense Lawyers**, the **Electronic Frontier Foundation**, and **The Sentencing Project**, I present to you their most recent response to the Commission's request for public comments as to how the Commission should respond to Section 225(b) of the Homeland Security Act of 2002, in particular, sentencing guidelines pursuant to 18 U.S.C. § 1030.

We would be happy to make available to you an electronic "pdf" version of this document, if you would like. Please advise us whether you would like us to email you this document as well.

We kindly thank the Commission for the opportunity to hear our comments in this matter.

Sincerely,

Jennifer Stisa Granick

JG:jsn
Enclosures

cc: Carmen D. Hernandez, Esq.
Lee Tien, Esq.
Malcolm C. Young, Esq.

[100]

The National Association of Criminal Defense Lawyers, The Electronic Frontier Foundation and The Sentencing Project write in response to the Commission's request for public comment about how the Commission should respond to Section 225(b) of the Homeland Security Act of 2002 (the Cyber Security Enhancement Act of 2002), Pub. L. 107-296, which directs the Commission to review and amend, if appropriate, the sentencing guidelines and policy statements applicable to persons convicted of an offense under 18 U.S.C. § 1030. We thank the United States Sentencing Commission for this opportunity.

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 even 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 crimes are already punished more harshly compared to other crimes for the reasons stated in these Comments.

The Sentencing Project is a Washington, D. C. -based 501(c)(3) non-profit organization, which promotes greater use of alternatives to incarceration and the adoption of sentencing policies, and practices which are fair and effective in reducing crime. Founded in 1986 to encourage improved sentencing advocacy by the defense, The Sentencing Project has become well known as a source of widely reported research and analysis on sentencing and other criminal justice issues. The range of these issues includes: the number of non-violent, low-level drug offenders in state prisons; crack-powder cocaine sentencing discrepancy in federal law; unwarranted racial disparity in the criminal justice system; the impact of the federally mandated ban on receipt of welfare benefits for women convicted of drug offenses; "Three Strikes" mandatory minimum sentencing laws; denial to nearly four million Americans of the right to vote following felony convictions; and, the significance of prosecuting children as adults.

The Sentencing Project's interests in the matter before the United States Sentencing Commission are to insure that federal penalties are not increased absent objective indications that an increase in penalties will reduce criminal computer fraud or "hacking," when other steps may provide a higher degree of public safety and corporate security, and when the rationale for increasing penalties may be based on a misperception of the nature and character of most crimes prosecuted through application of 18 U.S. C. Sec. 1030.

COMMENTS

Congress has directed the Commission to review the guidelines applicable to persons convicted of offenses under 18 U.S.C. section 1030 to ensure that the guidelines reflect the serious nature of such offenses, the growing incidence of such offenses and the need for an effective deterrent and appropriate punishment to prevent such offenses. Our comments submitted on February 17, 2003 express our position that current guidelines not only adequately reflect, but also in many cases overstate, the seriousness of the heartland 18 U.S.C. 1030 offenses. Further, current guidelines are rife with problems, especially surrounding the special definition of loss in computer crime cases.

In this set of comments, we respond to the Commission's questions regarding the special definition of loss for offenses involving unlawful access to a protected computer under Application Note 2(A)(v)(III) of §2B1.1. We also discuss the question of whether Congress's eight concerns are adequately addressed by the Guidelines. We believe that Congress's concerns are adequately addressed by the Guidelines, and that there are already provisions that enhance sentences for computer intrusion cases that involve intent to cause physical harm, interfere with government processes etc. These enhancements should only apply in cases where the

government has plead and proved beyond a reasonable doubt that the case involved particularly culpable intent.

We also recommend that the definition of loss be amended to more closely mirror the definition that applies to other economic crime cases. By defining loss as pecuniary harm reasonably foreseeable to the defendant at the time of the offense, the Commission can optimize the deterrent effect of sentencing while providing just punishment in accord with the defendant's culpability, rather than the victim's business choices about remediation efforts.

I. CURRENT SENTENCING LAW ADEQUATELY ADDRESSES THE EIGHT FACTORS IDENTIFIED BY CONGRESS

The Commissions' challenge is to establish a sentencing scheme for a single statute that penalizes computer intrusions ranging from website vandalism to cyberterrorism, and setting a wide range of statutory maximums, from one year to life. However, heartland computer crime case is analogous to economic fraud and most offenses are properly sentenced under guideline 2B1.1. We believe that guideline 2B1.1 should continue to address the heartland case of a computer intrusion that causes economic harm. Extraordinary cases where the government proves that the defendant intended cause physical harm or compromised national security may be enhanced pursuant to §3A4.1 (Terrorism), or be sentenced under a different guideline referred to in Appendix A, or receive an upward departure under existing guidelines such as § 5K2.2 (physical injury), § 5K2.3 (extreme psychological injury), or § 5K2.7 (disruption of government function).

We stress that the enhancements or guidelines specified below should only apply to computer crime offenses if the government pleads and proves special non-pecuniary harm as defined by the statute, or if the defendant admits such harm as part of a plea to the applicable subsection of section 1030. The applicable guidelines should be referenced by the statutory subsections in the Appendix, not cross-referenced in section 2B1.1. Cross references encourage courts to sentence computer criminals based on information about the crime that was not proven beyond a reasonable doubt at trial. This practice undermines certainty and predictability in calculating loss. Both promote deterrent effect and fairness in sentencing. Also, permitting enhancements only if warranted by the offense of conviction saves sentencing courts time, because they don't have to litigate at sentencing whether multiple special enhancements apply.

A. Whether The Offense Was Committed For Purposes Of Commercial Advantage Or Private Financial Benefit

The guidelines should not provide for a special enhancement for a computer criminal acting with a commercial purpose. Such an enhancement would result in double counting, as well as disproportionate sentencing as compared to other felony violations of section 1030.

Sections 1030(a)(2) and (c)(2)(A) provide that whoever intentionally accesses a computer without authorization or exceeds authorized access and thereby obtains information is subject to up to a year imprisonment. However, if the access was for purposes of commercial advantage or

private financial gain, then the maximum penalty is 5 years. 18 U.S.C. § 1030(c)(2)(B)(i). The guidelines do not provide an additional enhancement if this factor is present. Yet, the defendant's sentence will in fact be enhanced, because the one-year cap is removed. In most cases, based solely on the operation of other sentencing factors, the defendant will in fact receive increased punishment (i.e. more than one year) for acting with a commercial purpose. A special enhancement will amount to double punishment because the defendant would not only receive more than a year in prison but also an enhancement.

A special enhancement would also provide a disproportionate punishment for commercial motivation as compared to other felonious purposes. The section 1030(a)(2) misdemeanor offense also becomes a five-year felony if the access was in furtherance of any criminal or tortious act, or if the value of the information obtained exceeds \$5000. 18 U.S.C. §§ 1030(c)(2)(B)(ii)-(iii). The guidelines should not single out subsection (c)(2)(B)(i) for enhanced punishment over subsections (c)(2)(B)(ii)-(iii) especially because that motivation is not particularly depraved. Common business practices for the purpose of financial gain may be "unauthorized access" including sending unsolicited bulk email (America Online v. National Health Care Discount, 121 F.Supp.2d 1255, 1273 (N.D. Iowa 2000)), using automated search programs to collect even publicly available data (Register.com v. Verio, Inc., 126 F.Supp.2d 238, 251 (S.D.N.Y. 2000) [domain name information]; eBay v. Bidder's Edge, 100 F.Supp.2d 1058 (N.D. Cal. 2000) [internet auction information], EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577 (1st Cir.2001) [travel agent prices]) and placing "cookies" the computers of website visitors for purpose of monitoring their web activity (In re Intuit Privacy Litig., 138 F Supp 2d 1272 (C.D. Cal 2001); Chance v. Ave. A, Inc., 165 F.Supp.2d 1153 (W.D. Wash 2001). All have a commercial motivation, but none are particularly depraved as compared to other computer intrusions. We do not believe that a defendant acting with commercial motivation is more culpable than one acting in furtherance of another criminal or tortious act such that a special enhancement should apply.

B. Computer Used By The Government In Furtherance Of National Defense, National Security Or The Administration Of Justice

Section 1030(a)(1) prohibits obtaining classified information that would harm the United States or help a foreign power through unauthorized computer access and communicating that information to any person not entitled to receive it. There is a penalty of up to 10 years in prison for a first offense. 18 U.S.C. § 1030(c)(1)(A). Per the statutory appendix violations of this section are punished under guideline § 2M3.2. This guideline adequately addresses the seriousness of a § 1030(a)(1) offense.

For less serious cases that nonetheless harm a critical government computer, section 1030(a)(5)(A) prohibits transmission of code or unauthorized access that causes unauthorized damage. The definition of damage includes that which affects a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security. 18 U.S.C. § 1030(a)(5)(B)(v). This section prohibits actions that are less serious than those proscribed by section (a)(1), but possibly more serious than one which merely causes loss in an amount exceeding \$5000. However, not every violation of this section will be more serious.

The statute does not require proof that the defendant intended to damage government computer systems, only that the damage occurred. [If the damage was intentional, the defendant faces up to 10 years in prison. 18 U.S.C. § 1030 (c)(4)(A). If the damage was reckless, the defendant faces up to 5 years in prison. 18 U.S.C. § 1030 (c)(4)(B). If damage occurred without a specified intent, the defendant faces up to 1 year in custody. 18 U.S.C. § 1030 (c)(2)(A).] Nor does it require that the defendant's actions actually interfere with the administration of justice, national defense or national security. In rare cases when the defendant intends to and/or succeeds in interfering with these critical government functions, an upward departure may be appropriate under § 5K2.7 (Disruption of Governmental Function) or the § 3A1.4 (Terrorism). The § 3A1.4 enhancement is one of the most severe enhancements in the guidelines in that it enhances both the offense level and the criminal history under § 8C4.3 (Threat to National Security (Policy Statement)) may be warranted. We believe that this is sufficient.

However, if the Commission believes that §§ 5K2.7 or 3A1.4 are insufficient, then a targeted enhancement modeled on Guideline 3C1.1 may be appropriate. That guideline reads, "If (A) the defendant willfully obstructed or impeded, or attempted to obstruct or impede, the administration of justice during the course of the investigation, prosecution, or sentencing of the instant offense of conviction, and (B) the obstructive conduct related to (i) the defendant's offense of conviction and any relevant conduct; or (ii) a closely related offense, increase the offense level by 2 levels."

Similarly, the Commission may wish to increase the offense level by 2 levels if the defendant willfully obstructed or impeded, or attempted to obstruct or impede, the administration of justice or harming national defense or national security. However, this enhancement should only apply to convictions under section (a)(5)(A)(i) (intentional damage) that caused proven damage under (a)(5)(B)(v). It would overstate the defendant's culpability to apply this enhancement in cases where the damage to the government computers was not intentional and the defendant did not have the willful purpose of obstructing justice.

C. Malicious Intent To Cause Harm

The guidelines should not provide for a special enhancement for sentencing a computer criminal that acted with the malicious intent to cause harm. Such an enhancement would result in double counting.

Malice means that the defendant acted intentionally for the purpose of doing harm. Section 1030(a)(5)(A)(i), which provides that whoever knowingly causes the transmission of a program, information, code, or command and as a result of such conduct, intentionally causes damage without authorization may be punished up to 10 years in prison. 18 U.S.C. § 1030(c)(4)(A). Conviction of this subsection requires proof of malice. The guidelines do not provide an additional enhancement for conviction under this subsection. Yet, the defendant's sentence will in fact be enhanced, because the one-year or five year cap is removed when he is sentenced under section (a)(5)(A)(i). In most cases, based solely on the operation of other sentencing factors, the defendant will in fact receive increased punishment (i.e. more than one year) for maliciously causing harm. A special enhancement will amount to double punishment

because the defendant would not only receive both more than a year in prison but also an enhancement.

The Commission should not allow a sentencing enhancement based on this factor for conviction of any other subsection that does not require proof of malice at trial for the reasons stated above.

D. Violation Of Privacy Rights

The guidelines already take violations of privacy rights into account by providing for an upward departure if the offense caused or risked substantial non-monetary harm. For example, if a computer crime offense caused physical harm, psychological harm, or severe emotional trauma, or resulted in a substantial invasion of a privacy interest (through, for example, the theft of personal information such as medical, educational, or financial records) an upward departure may be warranted. Section 2B1.1, note 15 (A)(ii).

E. Intent Or Effect Of Significant Interference With Critical Infrastructure and Intent To Or Effect Of Threat To Public Health Or Safety Or Injury

There are multiple guidelines that take threat to public health or safety or injury into consideration. Section 1030(a)(5)(A) prohibits transmission of code or unauthorized access that causes unauthorized damage. The definition of damage includes that which causes a threat to public health or safety. 18 U.S.C. § 1030(a)(5)(B)(iv). This section prohibits actions that are possibly more serious than one that merely causes loss in an amount exceeding \$5000. However, not every violation of this section will be more serious. The statute does not require proof that the defendant intended to threaten public health or safety. [If the damage was intentional, the defendant faces up to 10 years in prison. 18 U.S.C. § 1030 (c)(4)(A). If the damage was reckless, the defendant faces up to 5 years in prison. 18 U.S.C. § 1030 (c)(4)(B). If damage occurred without a specified intent, the defendant faces up to 1 year in custody. 18 U.S.C. § 1030 (c)(2)(A).] Currently, the guidelines provide that an offense involving a conscious or reckless risk of death or serious bodily injury receives a two level enhancement and a minimum offense level of 14 under § 2B1.1(b)(11). It would overstate the defendant's culpability to apply a greater enhancement in cases where the threat of harm was not intentional.

In rare cases when the defendant intends to and/or succeeds in causing harm to public health or safety through unauthorized access to computers, other guidelines may apply. First, an upward departure under § 5K2.14 (Public Welfare) may apply. "If national security, public health, or safety was significantly endangered, the court may increase the sentence above the guideline range to reflect the nature and circumstances of the offense." Also, guideline § 3A1.4 may apply. That section provides that "If the offense is a felony that involved, or was intended to promote, a federal crime of terrorism, increase by 12 levels; but if the resulting offense level is less than level 32, increase to level 32." Also, "in each such case, the defendant's criminal history category from Chapter Four (Criminal History and Criminal Livelihood) shall be Category VI." This guideline is adequate to punish a violator of Section 1030 who intends to

harm the public safety or welfare. Furthermore, if the unauthorized access was a tool to commit murder, then the appropriate homicide guideline may apply if the indictment alleges and the proof at trial conforms with the elements of homicide See U.S.S.G. § 1B1.2 (instructions for selecting applicable guideline). It would overstate the defendant's culpability to apply this enhancement in cases where the threat to public safety was not intentional. Nor should the Commission cross-reference the homicide guidelines in section 2B1.1. This allows courts to impose greater sentences on defendants without proving the elements and mental state of those more serious crimes.

F. Level Of Sophistication Or Planning

The defendant's level of sophistication or planning is more than adequately accounted for in § 2B1.1(b)(8)(C), which provides for a two level increase and a minimum offense level of 12.

We believe that this adjustment often overstates the defendant's culpability. Computer crime offenders disproportionately receive a sentencing enhancement for special skill under § 3B1.3. Almost every computer offense inherently requires abuse of trust or special skill. Though the public uses computers, it is generally uninformed about computer security matters. A computer intruder must either use a password that permits access, leading to an abuse of trust adjustment, or know how to circumvent the password requirement, leading to a special skill adjustment. In its 1996 Report to Congress on the adequacy of federal sentencing guideline penalties for computer fraud and vandalism offenses, the Commission reported that 32.5% of all computer crime cases received an upward adjustment for abuse of position/special skill, as compared to 8.8% of white collar cases and 3% of all cases. Table 2.

Almost certainly, that percentage, and that discrepancy is higher today, if only because case law has supported a liberal application of the special skill adjustment in computer crime cases. In United States v. Petersen, 98 F.3d 502 (9th Cir. 1996), the Ninth Circuit held that the special skill adjustment only requires that the offender have skills not possessed by members of the general public. Special education or certification is not a prerequisite. While the Petersen court did not hold that a special skill adjustment would apply in every computer crime case, it greatly liberalized any limits on when the adjustment would apply. Anecdotal evidence suggests that a special skill adjustment is applied in almost every computer crime case today.

The additional special adjustment in § 2B1.1 for "sophisticated means" under § 2B1.1(b)(8)(B) further increases computer crime sentences. "Sophisticated means" means especially complex or especially intricate offense conduct pertaining to the execution or concealment of an offense. For example, in a telemarketing scheme, locating the main office of the scheme in one jurisdiction but locating soliciting operations in another jurisdiction ordinarily indicates sophisticated means. Conduct such as hiding assets or transactions, or both, through the use of fictitious entities, corporate shells, or offshore financial accounts also ordinarily indicates sophisticated means." § 2B1.1 Application Note 6(B). If this adjustment is also liberally applied to computer crimes, then the most basic computer crime offenses will be sentenced at a

minimum level 12. This results in a minimum sentence more than two times as high as the minimum sentence for the most basic economic crime.

The Commission should not provide for a special enhancement when the offense was committed for the purposes of commercial advantage or private financial benefit, or for malicious intent to cause harm. Enhancement for these factors would result in double counting and/or penalties disproportionate to the offense. The Commission should not provide for a special enhancement for offenses that affect a computer system used by a government entity in furtherance of the administration of justice, national defense, or national security. Current guidelines 2M3.2 and 8C4.3 are adequate. If the Commission believes otherwise, a targeted enhancement modeled on 3C1.1 should apply only to defendants that intentionally damage these government computers for the purposes of obstructing or impeding the administration of justice, or harming national defense or national security. There are already guidelines that take into consideration whether an offense involved a violation of privacy rights (Guideline 2B1.1, note 15(A)(ii), involved sophistication or planning (§ 2B1.1(b)(8)(C)), or intended to threaten public health or safety or cause injury (§§ 2B1.1(b)(11), 5K2.14, 3A1.4 and the homicide guidelines).

II. THE COMMISSION SHOULD ABANDON THE SPECIAL CALCULATION OF LOSS IN COMPUTER CRIME CASES AND ADOPT A DEFINITION LIKE THAT USED IN OTHER ECONOMIC CRIME CASES

Under the current sentencing law, the estimation of loss is the primary factor driving both economic and computer crime sentencing. Along with other relevant factors under the guidelines, loss should reflect the seriousness of the offense and the defendant's relative culpability. In economic crimes, the calculation of loss is generally limited to "reasonably foreseeable pecuniary harm." However, in computer crime sentencing, "actual loss includes the following pecuniary harm, regardless of whether such pecuniary harm was reasonably foreseeable: reasonable costs to the victim of conducting a damage assessment, and restoring the system and data to their condition prior to the offense, and any lost revenue due to interruption of service." USSG § 2B1.1 Application Note 2(A)(v)(III). The inclusion of unforeseeable pecuniary harms in the definition of loss, including "any lost revenue due to interruption of service" results in computer crimes being treated more harshly than other crimes. Additionally, the categories of harm described as loss are not easily assigned objective monetary value. As a result, the loss estimation for identical offenses can differ widely, resulting in grossly disparate sentences for identical conduct. For example, the cost of conducting a damage assessment depends more on the victim's actions than it does on the actions of the perpetrator or his intent to cause damage. A similar problem occurs with including any lost revenue due to interruption of service. Additionally, this definition of loss is susceptible to manipulation by victims, investigators and prosecutors.

We have identified two separate problems with the assessment of loss in computer crime cases. First, the definition of loss results in computer crimes being treated more harshly than other crimes by including unforeseeable losses. This problem can be alleviated by having the definition of loss for sentencing of computer crimes conform to the standard definition of loss for white-collar offenses. That definition includes only pecuniary losses that were reasonably

foreseeable to the defendant at the time of the offense and which were proximately caused by the defendant's actions. Second, the elements of loss are too difficult to accurately quantify. This problem is alleviated by adhering to an objective definition of loss that doesn't single out and encourage impractical measures of harm, but uses "reasonable foreseeability" as a guide to the sentencing court.

A. Definition Of Loss

First, the definition of loss for sentencing purposes should not mirror the statutory definition of loss. The statutory definition serves a different purpose from the definition used in sentencing. The statutory definition is a jurisdictional element that defines the point at which the federal government has a sufficient interest in prosecuting the matter. At trial, the prosecution must prove the requisite harm "beyond a reasonable doubt" since it is an element of the offense. The goals of sentencing, however, are "(a) to reflect the seriousness of the offense, to promote respect for the law, and to provide just punishment for the offense; (b) to afford adequate deterrence to criminal conduct; (c) to protect the public from further crimes of the defendant; and (d) to provide the defendant with needed educational or vocational training, medical care, or other correctional treatment in the most effective manner." 18 U.S.C. § 3553(a)(2). At least where the loss enhancement would not result in a "tail which wags the dog of the substantive offense," loss need only be proved by a preponderance of the evidence, U.S. v. Watts 519 U.S. 148, ___, 117 S.Ct. 633, 637, n.2 (1997), so long as the sentencing factor does not increase the maximum term allowed by law, Apprendi v. New Jersey, 530 U.S. 466 (2000).

The statute includes unforeseeable losses, a definition that fails to promote, and even denigrates, other goals of sentencing. Congress has identified unforeseeable losses as relevant to the seriousness of the offense, specifically the question of whether the offense caused sufficient harm that the federal authorities could prosecute it. However, sentencing based on unforeseeable losses does not promote respect for the law, provide just punishment for the offense, or properly deter criminal conduct. Citizens have less respect for the law when it produces unpredictable and inharmonious results, as the current definition does. Nor does the statutory loss definition result in just punishment. Sentences are disproportionate to the defendant's culpability because loss doesn't depend on either the defendant's actions or intent. Nor do sentences based on unforeseeable loss provide an optimum deterrent effect. Such sentences are "unforeseeable", not tied to the defendant's expectations. In fact, the sentencing scheme deters too much conduct, including common business practices. See February 19th comments, pp. 6-7, [Sending unsolicited bulk email (America Online v. National Health Care Discount, 121 F.Supp.2d 1255, 1273 (N.D. Iowa 2000)), using automated search programs to collect even publicly available data (Register.com v. Verio, Inc., 126 F.Supp.2d 238, 251 (S.D.N.Y. 2000) [domain name information]; eBay v. Bidder's Edge, 100 F.Supp.2d 1058 (N.D. Cal. 2000) [internet auction information], EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577 (1st Cir. 2001) [travel agent prices]), placing "cookies" the computers of website visitors for purpose of monitoring their web activity (In re Intuit Privacy Litig., 138 F Supp 2d 1272 (C.D. Cal. 2001); Chance v. Ave. A, Inc., 165 F.Supp.2d 1153 (W.D. Wash. 2001), shipping faulty software. See, e.g. Shaw v. Toshiba Am. Info. Sys., 91 F.Supp.2d 926 (E.D. Tex. 1999) [mailing floppy diskettes containing faulty microcode]; In re AOL, Inc. Version 5.0 Software Litig., 168 F.Supp.2d 1359 (S.D. Fla. 2001); Christian v Sony Corp. of Am., 152 F.Supp.2d 1184, 1187

(D.C. Minn. 2001).]

Therefore, for sentencing purposes, we believe that the definition of “loss” should include “only pecuniary losses that were reasonably foreseeable to the defendant at the time of the offense and which were proximately caused by the defendant’s actions.” This definition mirrors the one in use for economic crimes that the Commission recently adopted after much study and has several benefits over the current one. First, by including only pecuniary loss, it assists sentencing courts, which don’t have to value intangibles. Non-economic harms should be punished under a different section or be the basis for other adjustments as discussed above.

Second, “reasonably foreseeable” loss promotes uniformity in sentencing because similar offense conduct is likely to cause similar harm. Currently, the loss calculation is entirely in the hands of the victim. The assessment of damages depends more on the victim’s actions than it does on the perpetrator. The proposed definition resolves this problem by requiring that harm be reasonably foreseeable. By referencing the defendant’s point of view, and requiring that the defendant’s actions were the proximate cause of the loss, the definition ties the factor more closely to the defendant’s conduct and intent, better reflecting his culpability. The proposed definition also optimizes the deterrent effect without over-punishing.

Finally, loss should explicitly exclude costs of law enforcement investigation and prosecution.

B. Calculation of Loss

We believe that this new definition of loss will resolve a lot of the problems inherent in the current definition. The only reason why the current sentencing scheme hasn’t caused more of a stir is because courts haven’t been required to assess loss with any accuracy at all. The burden of proof in sentencing is by a preponderance of the evidence. Additionally, current guidelines advise that the sentencing court “need only make a reasonable estimate of the loss.” Guideline 2B1.1, Application Note 2(c). Proving something is a reasonable estimate by a preponderance of the evidence isn’t hard. As a result, judges aren’t worried about being reversed, and prosecutors are having an easy time arguing for high sentences. The goals of sentencing, however, are not served by the current definition.

The calculation of loss will still entail some evaluation of costs associated with damage assessment, costs of remediation, and lost revenue due to interruption of service. However, by requiring that these types of harms be “reasonably foreseeable”, the definition avoids the uncertainty and the manipulatability of the loss figure that characterizes the current sentencing scheme.

The current definition of loss includes any reasonable damage assessment conducted by the victim. Our proposed definition limits this discretion on the part of the victim by counting only “reasonably foreseeable” harm. It also distinguishes between doing an assessment for repair purposes and doing one that is forensically sound to preserve evidence for later prosecution. The proposed definition makes clear that costs associated with prosecution are not included in the definition of loss.

The current definition includes the cost of returning the system to the condition it was in prior to the incident. This definition is nonsensical, because the prior condition of the machine was insecure. No one wants to return their systems to that condition. Everyone wants to upgrade or repair the hole that allowed the defendant unauthorized access. The proposed definition makes clear that the defendant is responsible for assessment and remediation as a result of the hacking event, but not responsible for costs associated with upgrading systems and software that were insecure prior to the offense conduct.

The current definition includes "lost revenue due to interruption of service." Lost revenue 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. Some analysts estimated that Yahoo!'s loss would add up to millions of dollars. ZDNet News, February 7, 2000 <http://zdnet.com.com/2100-11-518359.html?legacy=zdn>. Sources quoted by the Industry Standard estimated that losses for Yahoo! and eBay would amount to 1.2 Billion dollars. February 11, 2000, <http://www.thestandard.com/article/display/0,1151,9703,00.html>. However, Yahoo! appears to have suffered no real loss of sales or advertising contracts as a result of the attack. For example, the company did not report these huge losses to the SEC.

Moreover, companies overestimate losses. For example, in U.S. v. Mitnick, the defendant accessed computers and viewed source code owned by the victim companies. The victims reported their estimate of the entire cost of research and development as their actual loss in the case. Sun Microsystems alone reported loss of 80 million dollars because the defendant saw the company's source code. However, the companies were not deprived of the use of that information, nor was it redistributed to competitors. Subsequently, Sun licensed the source code for \$100. See Wired News, How Much Damage Did Mitnick Do? May 5, 1999, <http://www.wired.com/news/politics/0,1283,19488,00.html>, See also, How Much Does Cybercrime Cost, ABC News, <http://abcnews.go.com/sections/tech/DailyNews/cybercrime990813.html>.

The proposed definition of loss will not depend on the victim's reasonable estimates, but on what was reasonably foreseeable to the defendant. Also, any calculation of loss should differentiate between temporary losses that are recoverable by the continued operation of the computer system of business, and permanent losses which can not be recouped. Defendants should not be held responsible for temporary losses that a company recovers simply by going back on line. This "limitation" should also remove the incentive for companies to overestimate losses.

C. Cap on Damages

We believe that the Commission should consider putting a cap on damages in cases where the defendant did not intend to cause harm under section 1030(a)(5)(A)(iii). Enhancing the sentences for the full amount of loss when the defendant did not intend to cause damage overstates culpability. The commentators suggest that the cap should be at no more than a four

level enhancement for loss. Starting with a base offense level of six, the sentencing court would most likely add two levels for sophisticated means, and four levels for loss. The heartland of section 1030 (a)(5)(A)(iii) cases for a first offender would then be sentenced between 10-16 months. We believe that this range accurately reflects the level of seriousness for this offense.

III. SENTENCING FOR VIOLATIONS OF 18 U.S.C. 2701

Violations of 18 U.S.C. section 2701 that are not committed for the purpose of commercial gain or in furtherance of any criminal or tortious act are misdemeanors, with a one-year maximum for a first-offense. We would recommend a simple guideline with a base offense level of six. For the offender with a prior, the criminal history category is likely to increase the sentencing range. Also, the court may depart upward if circumstances warrant. However, every violation of section 2701 will involve an invasion of privacy, so the Commission should make clear that that harm is taken into account in setting the base offense level.

///

///

///

///

///

///

IV. CONCLUSION

We encourage the Sentencing Commission to bring sentencing law for computer crime offenses in line with sentencing for other, similar economic crimes. We should eschew a strategy of creating a complicated sentencing scheme that applies many of the factors already considered in the guidelines in novel ways to the complicated area of computer crimes. This strategy interferes with the goals of sentences and creates a framework in which sentences are disproportionate to the defendant's culpability and chill legitimate computer security research, reporting and adoption of new, beneficial technologies.

Dated: March 17, 2003

Respectfully submitted:



Jennifer Sisa Granick
California Bar No. 168423
Center for Internet and Society
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

Malcolm C. Young, Executive Director
The Sentencing Project
514 - 10th Street, N.W., Suite 1000
Washington, D.C. 20004

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

**Comments of the United States Internet Service Provider Association
On Section 225 of the Homeland Security Act of 2002
Sentencing Guidelines
March 17, 2003**

The United States Internet Service Providers Association (US ISPA) is an organization comprised of major Internet Service Providers (AOL Inc., Cable & Wireless, eBay, EarthLink, Microsoft, SBC Communications, Teleglobe, Verizon Online, WorldCom, and Yahoo) throughout the United States. US ISPA welcomes this opportunity to submit written comments to the U.S. Sentencing Commission regarding Section 225 of the Homeland Security Act of 2002, sentencing guidelines applicable to defendants convicted of violations under the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. §1030.

Computer crime, including virus creation and distribution, computer intrusions, denial of service attacks, and theft of personal information, has continued to steadily increase over the last decade. Recent congressional testimony given by Assistant Attorney General Michael Chertoff, head of the Criminal Division at the Department of Justice, indicated that "there is no doubt that the number of crimes involving computers and the Internet is rising dramatically." For example, the CERT Coordination Center, which was created to warn network operators about computer attacks and viruses, received over 21,000 network crime incident reports last year. This is more than double the number of reports it received the previous year. Similarly, a survey conducted by the FBI and the Computer Security Institute recently revealed substantial increases in computer crime. Over 85 percent of the companies and government agencies surveyed reported computer security breaches within the preceding twelve months, up from 70 percent last year. Moreover, researchers at the University of California at San Diego recently reported a methodology that enabled them to count the numbers of denial of service attacks on the Internet; their research revealed that "4,000 attacks occur every week."

Some estimates of economic loss as a result of recent virus attacks add up to billions of dollars. Aside from the economic loss, our society's increasing dependence on computers means that the disruption of networks could seriously impair public safety, national security, and economic prosperity.

Today, however, sentences for violations of the CFAA are treated primarily as "white collar" fraud cases. Sentences are determined by calculating *actual or intended pecuniary harm*, something that is often difficult to quantify in the typical computer crime case. Under Guideline 2B1.1, significant economic loss is required before a defendant would even be eligible for imprisonment. In the case of the "Melissa" virus, a simple program that caused worldwide damage to millions of computers and computer systems, the perpetrator faced less than four years in prison even after proven damages of in excess of \$80 million. This lack of a significant criminal penalty eliminates the deterrent effect of a conviction, and makes the crime less likely to be prosecuted in the future. That is one reason that despite the enormous increase in the commission of computer crime, there is not a similarly large increase in prosecution of computer crime.

Newly emerging threats to the Internet, such as unsolicited bulk email, or spam, go largely unprosecuted because the type of harm spam causes is not currently addressed in the guidelines. Spammers send millions of unsolicited email messages that degrade and cripple entire email systems. However, the significant interference to the critical infrastructure caused by the abuse of spammers is not currently considered as a factor in the sentencing guidelines. Similarly, a common method for spammers to send bulk email, in an effort to by-pass spam blocking technology, is to steal personal email accounts and use their identities. The spammer's unauthorized access into the subscriber's account is a significant violation of the account holder's privacy rights. However, neither the violation of the individual's privacy rights by the spammer nor the spammers' financial gain from this illegal activity is taken into account in the sentencing guidelines, making prosecution for this type of offense extremely unattractive.

Moreover, the sentencing guidelines do not take into account the potential or actual harm caused by other types of crimes that may not cause economic loss, but have profound societal consequences: crimes that involve interference with important governmental functions, such as national security, national defense, and the administration of justice. For instance, viruses have attacked and taken down 911 operation centers in the past, knocking out the 911 emergency services for police stations and fire departments. This type of substantial harm to the public cannot be quantified in economic terms; and, if the perpetrators who created these viruses are finally caught, the disruptions they caused to these emergency services will probably not be used during their sentencing.

Cyber crimes should be viewed in the context of the overall incidence of the offenses and the extent to which they constitute a threat to civil peace and economic prosperity. The guidelines should not look just at the monetary damage a violation may cause, but at the important intangible loss of personal privacy and critical services that often results from cyber crime. Currently, the sentencing guidelines applicable to computer crime generally do not take into account these considerations.

We urge the Commission to amend the guidelines applicable to offenses under 18 U.S.C. §1030 to take full account of the eight factors listed in Section 225(b) of the Homeland Security Defense Act of 2002, particularly those factors that are not accounted for anywhere else in the applicable guidelines, such as whether the offense was committed for purposes of commercial advantage or private financial benefit; whether the defendant acted with malicious intent to cause harm in committing the offense; the extent to which the offense violated the privacy rights of individuals harmed; whether the offense involved a computer used by the government in furtherance of national defense, national security, or the administration of justice; whether the violation was intended to or had the effect of significantly interfering with or disrupting a critical infrastructure; and whether the violation was intended to or had the effect of creating a threat to public health or safety, or injury to any person. Economic loss alone does not adequately represent the threat to societal interests caused by computer crimes.

February 01, 2003

Re: U.S. Sentencing Commission
Proposal for Amending the
U.S. Sentencing Guidelines

Issues Addressed

- * 21 USC 851
- * Criminal History Points

Sentencing Commission,

The issues to be addressed is of great importance and must be addressed soon. If these issues are continued to be over looked the Federal Bureau Of Prison System will continue to become over crowded with non-violent offenders; yes convicted felons although contrary to belief given a chance these people can become productive citizens while lifting the burden of housing these inmates off the tax payers budget in many many ways.

§851

Under the current law §851 as with many Federal Laws the United States Attorney has the discretion on which statute or code is applied and why it is applied in certain cases. Under §851 the defendant is subjected to increase punishment by reason of prior conviction (only one being required) the court shall proceed to impose sentence upon him as provided by this statute; 21 USC 851(d)(1). This section reads as though the judge has some if any discretion when in fact the hands of the judge are tied as with many of the Federal Statutes now in effect. The issue of the §851 should be considered for amendment to add a more stringent check system. The statute has no mitigating factors i.e. murder, guns, or victims ect.. The U.S. Attorney

(1)

[116]

has no checks and balance system when applying the §851 to enhance a sentence, which in many cases are more than excessive to begin with. In 96% of the cases the §851 is applied their involves a minimum mandatory set by the sentencing guidelines that the Judge must apply (again hands are tied). The §851 enhancement is used without any mitigating factors to turn the minimum mandatory sentence of TEN years into 20 yrs. and the minimum mandatory of TWENTY years into a MANDATORY LIFE sentence with on chance of parole. These are the affects of the §851 this is done all without any mitigating factors, no checks and balances for the U.S. Attorney while the hands of the judge are tied.

In 99% of cases the §851 is applied the U.S. Attorney offered a plea deal; 100% of the cases the deal was for sentences of 50% below the minimum mandatory. Because the defendant choice was to exercise his/her right to a trial in hopes of proving their innocents the 851 was applied for an enhanced sentence apon conviction. In 100% of these cases the §851 was applied only days most times less than 24 hours before the jury was to be selected, so this issue boarders the line of prosecutorial vindictiveness; take the plea or get excessive time innocent or not!

The bottom line here is the use of the §851. This statute serves the purpose of enhancing already excessive sentencing, causing double punishment for past state charges that may or maynot have been found to be convictions in the state courts, is used along with other enhancing statutes (criminal history points), and is a tool for prosecutors to punish people for exercising their rights by using the Justice System. This Statute is flawed as are many.

The Judge has no dicretion on the application of the §851 or the Minimum Mandatory sentences to be applied by the U.S. Attorney. In two out of 4 cases the Felony used to enhance the sentence

adjudication was withheld; no guilt was established. So contrary to the U.S.S.G. the U.S. attorney say's it's legal to apply the §851 to non-convictions in the eyes of State Court (an issue for the appeals court).

* Criminal History

Under §4A1.2 Definitions and Instructions for Computing Criminal History

(a) Prior Sentence Defined

- (1) The term "prior sentence" means any sentence previously imposed upon adjudication of guilt, whether by guilty plea, trial, or plea of nolo contendere, for conduct not part of the instant offense. U.S.S.G. 2002 p.315

Under this text according to the U.S.S.G. prior sentence is stated to be a conviction "imposed upon adjudication of guilt" by any rout. Even as the sentencing guidlines states this in plain english it is being used as though any sentence is used without established guilt.

While under §4A1.2(c) Sentences Counted and Excluded

Sentences for all felony offenses are counted. Sentences for misdemeanor and petty offenses are counted, except as follows:

- (1) Sentences for the following prior offenses and offenses similar to them, by whatever name they are known, are counted only if (A) the sentence was a term of probation of at least one year or a term of imprisonment of at least thirty days, or (b) the prior was similar to an instant offense: See U.S.S.G. 2002 p. 316

4A1.2(c) context is stating that sentencing must have been a term of at least one year or 30 days imprisonment. I am finding that under §4A1.1(c) points are being added for misdemeanors where no guilt was established nor was the requierments met to warrent points under this section. In 100% of the case researched the Probation officer in preparing the PSR added points for misdemeanor cases that did not met the critirrior under any section of the U.S.S.G.. Due to the mis-interpretation of the U.S.S.G. points are being added and more time is being added and more defendants are spending more time being housed on the tax payers dollar.

Prison alternatives would save tax payer millions of dollars. While States such as Kentucky, Michigan, Connecticut, Louisiana, Mississippi and North Dakota, Texas, Oregon, Idaho, California and Arkansas are using alternatives like early release for non-violent inmates to ease the budget; while addressing the legitimate safety concerns of citizens and the need to help offenders take control of their lives to become productive citizens of society.

While Michigan signed into law a bill repealing the States mandatory minimum sentencing laws for drug crimes (non-violent), thus giving the judge the discretion to sentence offenders to probation or jail time as see fit. These steps reduces the number of first time offenders going to prison, thereforesaving the tax payers millions of dollars.

The Federal system is currently home to over 170,000 men/women, 73% of these offenders are non-violent offenders. The average sentence is 120 months for non-violent crimes, the most popular charge is currently conspiracy this charge carries a minimum mandatory of TEN, 20, LIFE and due to this the system is over crowded with non-violent offenders at the cost of housing each offender for one year at 22K. With the population of the BOP the budget from year to year is almost 3.74BILLION you do the math if it don't help it does not make sense.

This is a citizens reply to the proposal for amending the U.S. Sentencing Guidelines. Give those that are non-violent offenders a chance to re-enter society and give back to their community and provide for the children and families that are innocent victims of their crimes. Any changes to the U.S.S.G should assist in releasing those that have been in the prison system for far to long because of the minimum mandatroy sentencing that are way to excessive.

Thank you for taking time out to review the issues . Being a citizen of the United States gave me this chance to address these issues with you. The Education System, Health System and the Welfare System is suffering so why are tax dollars going to the BOP when they can used for the well being of the citizens whom are paying the taxes.

Citizen of the U.S.A.

(5)

[120]

SITE OF RESEARCH:

Clerk of Court @
Federal Courthouse Square
301 North Miami Avenue, Rm. 105
Miami, FL 33128-7788

611 United States Courthouse
80 North Hughey Avenue
Orlando, FL 32801

2211 Richard B. Russell Federal Building
75 Spring Street, S.W.
Atlanta, G.A. 30303

210 Charles R. Jonas Federal Building
401 West Trade Street
Charlotte, N.C. 28202

Strom Thurmond Federal Building
1845 Assembly Street
Columbia, SC 29201

Albert V. Bryan United States Courthouse
401 Courthouse Square
Alexandria, VA 22314

Federal Prison Journal 2002

United States Sentencing Guidelines 2002

(I)

[21]

JANUARY 30, 2003

U.S. SENTENCING COMMISSION
ONE COLUMBUS CIRCLE N.E.
SUITE 2-500, SOUTH LOBBY
WASHINGTON, DC 20002-8002

PUBLIC COMMENT:
CONCURRENT SENTENCES

COULD THE SENTENCING COMMISSION TAKE IN CONSIDERATION, AND HELP THE FELONS THAT MOST NEED A CONCURRENT SENTENCE. THE FELONS THAT GET PUNISHED DOUBLE FOR THE SAME STATE CHARGE! THE FELONS THAT GET THERE FEDERAL CHARGE ENHANCED UNDER 4B1.2 BECAUSE OF THERE STATE CHARGE, THEN RUN CONSECUTIVE TO THE SAME STATE CHARGE! THIS 4B1.2 SHOULD BE ONE OF THE MECHANISMS THAT TRIGGER A CONCURRENT SENTENCE. THE 4B1.2 IS COUNTED IN THE BASE OFFENSE LEVEL IN CHAPTER 4. THEY ARE THE MOST NEEDING THE CONCURRENT SENTENCE AND WOULD STOP THE DOUBLE COUNTING ON THEM FOR THE SAME STATE CHARGE. IT IS INCORPORATED IN THE BASE OFFENSE UNDER 4B1.2. SO THEREFORE IT SHOULD BE ADDED IN BESIDE RELEVANT CONDUCT 1B1.3 UNDER 5G1.3(B).

I ALSO READ RUGGIANO V. REISH 307 F3D 121. I AGREE WITH THAT COURTS SHOULD HAVE AUTHORITY UNDER 5G1.3(C) IN CASES THAT UNDER 4B1.2. KEEP THE DEFENDANT FROM BEING PUNISHED DOUBLE.

THANK YOU,

Harold Gary

JANUARY 30, 2003

U.S. SENTENCING COMMISSION
ONE COLUMBUS CIRCLE N.E.
SUITE 2-500, SOUTH LOBBY
WASHINGTON, DC 20002-8002

PUBLIC COMMENT:
CONCURRENT SENTENCES

COULD THE SENTENCING COMMISSION TAKE IN CONSIDERATION, AND HELP THE FELONS THAT MOST NEED A CONCURRENT SENTENCE. THE FELONS THAT GET PUNISHED DOUBLE FOR THE SAME STATE CHARGE! THE FELONS THAT GET THERE FEDERAL CHARGE ENHANCED UNDER 4B1.2 BECAUSE OF THERE STATE CHARGE, THEN RUN CONSECUTIVE TO THE SAME STATE CHARGE! THIS 4B1.2 SHOULD BE ONE OF THE MECHANISMS THAT TRIGGER A CONCURRENT SENTENCE. THE 4B1.2 IS COUNTED IN THE BASE OFFENSE LEVEL IN CHAPTER 4. THEY ARE THE MOST NEEDING THE CONCURRENT SENTENCE AND WOULD STOP THE DOUBLE COUNTING ON THEM FOR THE SAME STATE CHARGE. IT IS INCORPORATED IN THE BASE OFFENSE UNDER 4B1.2. SO THEREFORE IT SHOULD BE ADDED IN BESIDE RELEVANT CONDUCT 1B1.3 UNDER 5G1.3(B).

I ALSO READ RUGGIANO V. REISH 307 F3D 121. I AGREE WITH THAT COURTS SHOULD HAVE AUTHORITY UNDER 5G1.3(C) IN CASES THAT UNDER 4B1.2. KEEP THE DEFENDANT FROM BEING PUNISHED DOUBLE.

THANK YOU,

Sonya Gargent

JOHN J. SHORTER

Reg. No. 03970-027, P.O. Box 5000, Greenville, Illinois 62246

February 21, 2003

Michael Courlander,
Public Affairs Officer
U.S. Sentencing Commission
One Columbus Circle, NE
Suite 2-500
Washington, DC 20002-8002

RE: Public Comment On Proposed Amendment(s): §5G1.3(b)
And Its Retroactive Application

Dear Mr. Courlander:

I am writing as someone who will be directly affected by the proposed amendments to §5G1.3(b), assuming retroactivity. I have spoken to and written your office on several different occasions regarding the unjust "Crack-Law" and most recently the 2002 Application Note 7 (Downward Departure Provision) to the Commentary of §5G1.3(b). (See your attached response.)

My Brief Case History

I have been incarcerated since April 11, 1990, shortly after my 22nd birthdate. I am a first time non-violent "Crack-Law" offender serving a 30 year concurrent sentence. Prior to my federal arrest I was serving a 6 year state (Fort Wayne, Indiana) sentence for the same offense. A fact that has been repeatedly acknowledged by my federal judge, the government and the probation department. I was taken in to federal custody on May 6, 1993, prior to the discharge of my state sentence. Unfortunately, I was again convicted and later sentenced federally to 30 years without receiving an adjustment for the 6 years I completed on the related state case.

At the time of my federal sentencing the 6 year state sentence had been discharged and, as a direct result, the judge refused to apply §5G1.3(b) ('94 version), citing a lack of authority. However, he did instruct me to take the issue to the Bureau of Prisons ("BOP") which, I did. And the BOP has steadfastly denied my repeated requests for the proper adjustment of my sentence since 1994. Therefore, my ultimate sentence is: 6 years state plus 30 years federal with a 5 year Supervised Release Term (41 years); for a first time non-violent offense.

2002 Application Note 7

In the previous amendment cycle the Commission issued a

a clarifying amendment to §5G1.3(b). Therein, agreeing with United States v. Blackwell, 49 F.3d 1232, 1241-42 and n.20 (7th Cir. 1995). This case held and the Commission agreed, that "distinguishing between two defendants merely by virtue of their sentencing dates appears contrary to the Guidelines 'goal of eliminating unwarranted sentence disparities.'" In addition it was rightly noted that "it perhaps could be argued that applying the guidelines to undischarged sentences but not to discharged sentences lacks a rational basis and therefore violates the Constitution." The acceptance of these facts by the Commission clearly argues in favor of retroactive application. This is true simply because if it is unjust and unconstitutional now, then it was unjust and unconstitutional then and the U.S. Constitution remains unchanged.

2003 Proposed Amendment To §5G1.3(b)

I am very pleased and relieved that the Commission is again addressing this important issue to achieve the Guidelines stated goals. Upon reviewing the amendment options, I believe that "Option Two B" is more appropriate. This option gives judges more latitude to fashion fair sentences in particular cases. In addition I assert that the application of this option should be mandatorily applied [shall]. Therefore, judges will not be unnecessarily restricted and at the same time required to apply the fairness this amendment permits.

In my particular case either option would apply, however, the additional specific requirement that any increase be directly relevant is unnecessary. Any fact that increases the instant offense should be considered in tandem with the instant case. This would promote fairness and give judges the option to more fully exercise the authority it has been granted by the Constitution.

Retroactivity of 2003 Proposed Amendment

The importance of the recognition that §5G1.3(b) should be overhauled in the suggested manner is proof positive that it should be extended to every case it affects. In my limited research on the effect of this amendment, I have found that it will not open the flood gates and release thousands of underserving defendants. Using my specific case as an example the direct affect of retroactively applying this amendment would be as follows:
6 years state - 30 years federal = 24 years to serve with an additional 5 years of supervised release.

The judge in my case specifically instructed me to address my issue with the BOP in the first instance but the BOP refuses to adjust my sentence. Should I not have an opportunity to redress the unjust sentence I received? The judge in my case stated on numerous occasions, during my post conviction proceedings, that he believed the sentence was extremely severe but that his hands were tied by the Guidelines. Even with the reduction in my sentence I would still be required to serve over 20 years in prison. Twenty years or more of incarceration is very harsh for a first time non-violent offender.

Issue For Comment: §5G1.3(c)

I address this issue in light of the potential effect it could have on §5G1.3(b). I believe the Commission should address this issue and resolve it in favor of the holdings of Ruggiano v. Reish, 307 F.3d 121 (3d Cir. 2002). I believe the case itself articulates the specific reasons of why and how this issue should be resolved. Infact I submit that the courts should be able to grant "credit" for time served in state prison for an undischarged sentence, in addition to running the federal sentence concurrently with the remaining portion of a defendant's preexisting sentence, as well as be able to grant this credit for discharged sentences.

Ruggiano exhausted his BOP remedies first and then filed a § 2241 petition with district court. I believe that this option should be available to §5gl.3(b) situations as well, especially if the Commission does not specifically make the amendments to §5G1.3(b) retroactive.

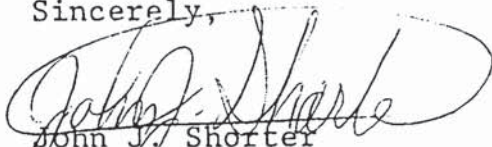
The current proposed amendments to §5G1.3 are substantial in comparison to last year's 2002 Application Note 7 (Downward Departure Provision), which was merely clarifying. The Commission's imposed authority should be used to address and apply the Guidelines in an even-handed manner. As a result, I urge the Commission to considers the comments offered by someone who's life and family's life will be tremendously affected by the actions taken on these proposed amendments.

Conclusion

In closing, I would like to thank you for the opportunity to voice my comments and sincere passions on the above issues. I pray that compassion would continue to overrule the political roadblocks which may be erected by some of those who do not face the affects of this concern directly.

Also, if this commission would like for me to submit any specific information that it deems helpful, please do not hesitate to contact me or even consider my signature below as permission for the Commission to use my specific sentencing information any way it seems appropriate.

Sincerely,



John J. Shorter
F.C.I. Greenville
P.O. Box 5000
Greenville, IL
62246

UNITED STATES SENTENCING COMMISSION
ONE COLUMBUS CIRCLE, N.E.
SUITE 2-500, SOUTH LOBBY
WASHINGTON, D.C. 20002-8002
(202) 502-4500
FAX (202) 502-4699



October 10, 2002

John J. Shorter
Reg. No. 03970-027
P.O. Box 5300
Adelanto, CA 92301

Dear Mr. Shorter:

Your letter to the Commission has been referred to me for response. The recent amendment proposed to U.S.S.G. §5G1.3 has not been authorized by the Commission for retroactive application. I have no further information concerning the Commission's April 15, 2002 recommendations to Congress on crack cocaine sentences.

Very truly yours,

A handwritten signature in cursive script that reads "Michael Courlander".

Michael Courlander
Public Affairs Officer

Craig Patterson
Reg. No. 09385-045
USP Leavenworth
Post Office Box 1000
Leavenworth, Kansas 66048
Mrs. Diana Murphy - Chair

Re: "Crack" Cocaine Sentencing Policy

February 18, 2003

Dear Mrs. Murphy:

I am writing you after recently reading the report and recommendations that was filed to Congress (May 2002) dealing with the cocaine and "crack" cocaine sentencing policy.

Being a first time non-violent drug offender, I was very disturbed by your sentencing guideline results. I believe I speak on the behalf of all non-violent drug offenders, which reaches in the tens of thousands, when I address this concern.

What troubles me and many others, is the five(5) kilogram gap (between 2.5 and 7.5 kilos) that comes into play at level 38 and 36 with your new model guideline that will apply with changing the 100-1 ratio to 20-1 dealing with "crack" cocaine. Must I also imply that it is this street word - "crack" - that has influenced the minds of the Sentencing Commission and Congress to summons these heinous forms of punishment.

If the 100-1 ratio is unfair, then 20-1 ratio must also be unfair. I ask you a question, why is "crack" the only illegal drug with a spacious ratio? Since your report shows that it is unjust to Blacks and Latinos, it would be just to say that race is the reason why.

The concern is great because with changing the "crack" law to 20-1, there will still be tens of thousands of non-violent drug offenders that will not feel any effect of the change, due to the five(5) kilogram differential.

To my understanding, these laws were inacted mainly for "Drug Kingpins". Ask any Black or Latino who has been convicted either with conspiracy of, or possession of five(5) to ten(10) kilograms of "crack" or cocaine, is that person considered a "Kingpin". The answer is obviously NO! Inner City street dealers are being handed down sentences that should normally be awarded to suppliers that are shipping in hundreds upon hundreds, to thousands to tons of "powder cocaine".

It seems so easy for the Commission to present to Congress a law without any sufficient research of the outcome of the law or background of the problem, but after seventeen(17) years, cannot administer a cure. I question all of the Sentencing Commission to delve deeper into the fairness, reality, and rationality to obtain a result that aligns itself in truth. There is a short way to this destination, and that is the RIGHT WAY

Please find enclosed a copy of a motion that was prepared and filed in the Supreme Court by some 26 prisoners. This motion was denied review, i.e. the Supreme Court chose to not review the issues.(merits never addressed)

Thank you for earnest and sincere consideration of this matter.

available
upon request
-on file with
Public Affairs

Sincerely,

Craig Patterson
Craig Patterson
Reg. No. 09385-045
USP Leavenworth
Post Office Box 1000
Leavenworth, Kansas 66048

February 18,2003

CC: Rueben Castillo - Vice Chair
William K. Session, III - Vice Chair
John R. Steer - Vice Chair
Sterling Johnson, Jr. Commissioner
Micheal E. O'Neill - Commissioner