



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

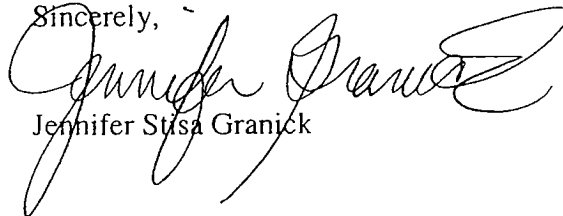
Dear Ms. Hickey:

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.

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 manipulability 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.

///

///

///

///

///

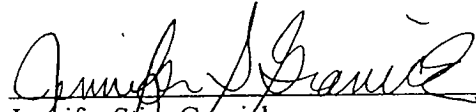
///

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