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 event the least among us who may be accused of wrongdoing; compassion for witnesses and victims of crime; and just punishment for the guilty.

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

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

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

EFF has been deeply concerned about the criminalization of online behavior since its inception. The founders intended EFF to bring balance and reason to law enforcement in cyberspace. One incident that brought this need home was a 1990 federal prosecution of a student for publishing a stolen document. At trial, the document was valued at $79,000. An expert witness, whom EFF helped locate, was prepared to testify that the document was not proprietary, and was available to the public from another company for $13.50. When the government became aware of this information through defense's cross-examination of government witnesses, it moved to dismiss the charges on the fourth day of the trial.

Accordingly, EFF is very concerned that the Sentencing Commission act very carefully with regard to computer crime sentencing. We believe that those convicted of computer 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 rational 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. Section 1030.

COMMENTS

Congress has directed the Commission to review the guidelines applicable to person 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. We write in response to the Sentencing C request for comments because we believe that the guideline range should not be increased.

Current guidelines not only adequately reflect, but also in many cases overstate the seriousness of 18 U.S.C. 1030 offenses. Section 1030 proscribes offenses that range in seriousness from misdemeanors to threats to national security. However, the heartland section 1030 violations are white collar fraud or insider misappropriation of information cases that should be treated comparably to other white collar fraud cases. Current section Three guidelines would substantially enhance sentences in rare cases of “cyberterrorism”. Also, there has not been a significant increase in the commission of section 1030 offenses over the past five years that requires increased sentencing. Further, increased sentences will not deter terrorists, who may be willing to die for their cause, but may deter legitimate business innovation and practices as well as important computer security research and vulnerability testing.

In fact, current guidelines are rife with problems, mostly surrounding the special definition of loss in computer crime cases. The definition includes unforeseeable losses that are wholly defined by the victim's behavior rather than the defendant's actions. Sentences that are widely disparate for identical offenses, easily manipulatable, and that do not accurately reflect the defendant's culpability result.

I. THE GUIDELINE RANGE SHOULD NOT BE INCREASED

A. The Seriousness of the Offense is Comparable to Other Fraud or Theft Cases, not Offenses to the Person or Terrorism Cases

The typical computer crime offense involves a disgruntled current or former employee misusing company computers. The Department of Justice maintains a non-exhaustive chart of computer crime cases on its website at www.cybercrime.gov/cccases.html. The chart has 59 entries, representing 55 unique cases. Of those, the chart describes sixteen of the defendants as employees of the victim company. Review of the linked DOJ press releases shows that an additional nine defendants were also employees or independent contractors of the victim. (Luckey, Blum, Leung, Farraj, Scheller; Brown; Carpenter; Dennis, and Alibris.) Thus, almost half of the cases in the table are readily identifiable as involving disgruntled insiders. In forty three of the fifty nine entries, the defendant caused harm to a solely private interest. Only fifteen of the cases involve harm to a public or public and private interests. Only one case, where the defendant was a juvenile, involved a threat to safety. This small set of data shows that the heartland computer crime case involves disgruntled employees causing harm to private companies.

Of course, this cursory analysis depends entirely on a small set of data selected for publication by the Department of Justice. Defendants in the listed cases may eventually be acquitted, or the nature of the case may not be fully or accurately reflected in the press releases, or by the inclusion of the case in the table. For example, United States v. Alibris involved allegations that a company that provided email services to subscribers violated18 U.S.C. 2511 (interception of electronic communications), not 18 U.S.C. 1030. Additionally, the district court recently ruled in the Alibris case that the company's actions were not prohibited by section 2511. U.S. v. Councilman, U.S. District Court for the District of Massachusetts, 01-CR-10245-MAP (February 12, 2003), available at http://pacer.mad.uscourts.gov/dc/cgi-bin/recentops.pl?filename=ponsor/pdf/councilman2.pdf. Also, not all section 1030 cases are included in the table – for example, U.S. v. Middleton, 35 F.Supp.2d 1189 (ND Cal 2002), 231 F.3d 1207 (9th Cir. 2002) and U.S. v. Sablan, 92 F.3d 865 (9th Cir. 1996), in which both defendants were disgruntled (ex-) employees.

Based on the available information the typical section 1030 offense appears to be comparable to a white collar fraud. We urge the Commission to treat section 1030 offenses similarly, absent other considerations. Since the Commission recently amended the guideline applicable to economic crimes (2B1.1), there is no reason now to increase penalties further for computer crime cases.

B. There are Already Guidelines that Can Apply to Terrorism Offenses and Offenses to the Person that Fall Under Section 1030

To date, there are no reported incidents of terrorists attempting to harm the health and safety of individuals through unauthorized computer access. However, in an abundance of caution, Congress amended section 18 U.S.C. 1030 to especially prohibit this type of offense and to proscribe a term of up to life in prison. 1030(a)(5)(A)(i). This should not inspire the Commission to increase punishment under the guidelines for the heartland of section 1030 cases, which, as shown above, primarily involve employment disputes. There are already guidelines that apply to attempts to commit bodily harm, as wells as the rare terrorist computer crime offender. Guideline §3A1.4(a) provides "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." This guideline is adequate to punish a violator of Section 1030 who acts with terroristic intent.

C. Incidents of Section 1030 Violations are Not Increasing

Current statistics do not show an upward trend in section 1030 violations. We would expect to see some increase in violations as more people use computers and become connected to the Internet. We would also expect to see increased convictions as law enforcement becomes better trained and puts more resources into computer crime investigation and the formation of high tech crime task forces. However, the actual incidence of computer crime prosecutions is little more than 100 per year.

The Transactional Records Access Clearinghouse (TRAC) located at Syracuse University makes targeted FOIA requests to collect, among other things, statistics on DOJ enforcement. For each incident referred to the DOJ, TRAC records a host of information, including referral date and agency, lead charge, disposition date and type, and prosecution filing date or declination reason. TRAC defines enforcement data as:

> Fraud involving violations of 18 U.S.C. 1030 or 2701 et. seq., computer "bulletin boards" and other schemes in which a computer is the target of the offense, including when charged as violations of 18 U.S.C. 1343, 2314, or 2319 e.g., computer viruses or where the defendant's goal was to obtain information or property from a computer or to attack a telecommunications system or data network. (All such cases are national priorities.)

Program Category, at http://tracfed.syr.edu/help/codes/progcode.html (last visited June 19, 2002). Further information about TRAC's enforcement database resides at http://tracfed.syr.edu/index/cri/cri_help_index_pros.html/

Data obtained by the commentators on computer crime prosecutions shows a steady increase in referral for prosecution and also in prosecutions. However, the number of prosecutions remains low and shows only slow growth. Though there was a dramatic increase in referrals from 1999 to 2000, there was also a large increase in the number of prosecutions declined. The actual conviction rate increased, but from only 72 convictions to 107 between 1999 to 2001.

	Fiscal Year									
	1992	1993	1994	1995	1996	1997	1998	1999	2000	2001
# of referrals for prosecution	115	126	155	201	197	292	417	497	807	853
# of referrals disposed of	69	100	133	137	172	178	253	360	491	631
# of referrals with prosecution declined	53	68	110	105	126	125	196	271	393	496
# convicted after prosecution	12	26	18	23	33	37	47	72	81	107
# not guilty after prosecution	4	6	5	9	13	16	10	17	17	28

In comparison, in 1999, 38,288 drug offense cases were referred for prosecution. That same year, 29,306 people were charged with a drug offense. Between 1984 and 1999, the number of defendants charged with a drug offense in Federal courts increased from 11,854 to 29,306. United States Department of Justice, Bureau of Statistics, Special Report, Federal Drug Offenders, 1999, with Trends 1984-1999, available at http://www.ojp.usdoj.gov/bjs/abstract/fdo99.htm. In 1999, United States Attorneys chose to prosecute over 88% of suspects referred for drug crime.

In fiscal year 1998, the DOJ disposed of 253 computer crime referrals. Some of these referrals reached the DOJ in earlier years, but the DOJ disposed of all of them between October 1, 1997 and September 30, 1998. Of the 253 dispositions, 196 (77%) were declined prosecutions while 57 (23%) ended in court. Forty-seven dispositions (19%) were due to a guilty verdict or an appellate court victory, and 10 (4%) were due to acquittals or dismissals. Of the 47 found guilty in court, 20 (43%, 8% of all disposals) received prison sentences. In 2001, the DOJ disposed of 631 computer crime referrals. Of these, 496 (78%) were declined prosecutions, while 135 (21%) ended in court. One hundred seven dispositions (17%) were convictions and twenty eight (4%) were due to acquittals or dismissals.

The Department of Justice declined prosecution for the following reasons.

Declination Reason	*Number*	*% of Declinations*	*% of Total Dispositions*
Lack of evidence of criminal intent	27	13.78%	10.67%
Weak or insufficient admissible evidence	34	17.35%	13.44%
Suspect to be prosecuted by other authorities	23	11.73%	9.09%
No federal offense evident	21	10.71%	8.30%
Minimal federal interest or no deterrent value	19	9.69%	7.51%
No known suspect	17	8.67%	6.72%
Juvenile suspect	10	5.10%	3.95%
Agency request	10	5.10%	3.95%
Civil, administrative, or other disciplinary alternatives	6	3.06%	2.37%

Office policy (fails to meet prosecutive guidelines)	6	3.06%	2.37%
Jurisdiction or venue problems	5	2.55%	1.98%
Pre-trial diversion completed	5	2.55%	1.98%
Lack of investigative or prosecutive resources	4	2.04%	1.60%
Witness problems	3	1.53%	1.19%
Suspect being prosecuted on other charges	3	1.53%	1.19%
Other	13	6.63%	5.15%

Thus, a review of the statistics suggests that the incidence of computer crime is very low, and, while slowly increasing, is not increasing at a rate that currently justifies instituting harsher penalties in light of the other considerations. Also, a significant number of these offenses involve disgruntled former employees, and criminal conduct of similar seriousness. The statistics on declinations suggest that the Assistant United States Attorneys do not believe that the damages and consequences of computer crimes reported to the Department are serious enough to merit a higher prosecution rate. Similarly, these crimes do not merit an increase in sentence length.

D. Deterrent and Chilling Effect

Nor should the Commission increase computer crime penalties as a deterrent unless statistical evidence shows that those convicted of section 1030 offenses re-offend at a statistically significant rate. In 1996, the Commission concluded that "existing data do not permit the Commission to draw any firm conclusions regarding the deterrent effect of existing guideline penalties for these computer-related crimes." Report to the Congress: Adequacy of Federal Sentencing Guideline Penalties for Computer Fraud and Vandalism Offenses, p. 3. Similarly, The Commission should examine whether new data allows any new conclusions.

Greater penalties are dangerous. They may chill legitimate computer research, business development, and reporting on security vulnerabilities. Section 1030 generally prohibits "unauthorized access" to computer systems, while subsection 1030(a)(5) prohibits the "transmission" of harmful code. These are broad definitions. Case law shows that a wide range of common business practices have been challenged in civil suits under section 1030. Though these cases are civil, and though some of the business practices were held not to be actionable, the Commission should view these cases as a cautionary tale. First, there is no difference between the definition of civil and criminal offenses under section 1030, so the judicial interpretations of the statute apply in both situations. Second, in cases where the plaintiff's case failed, it was always for failure to show jurisdictional damages of greater than $5000, rather than failure to show that the contested business practice was in fact "unauthorized access" or an illegal "transmission."

Common business practices that may be "unauthorized access" or illegal transmission 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 (CD Cal 2001); Chance v. Ave. A, Inc., 165 F.Supp.2d 1153 (WD Wash 2001).[1]

Additionally, companies like AOL and Toshiba are potentially liable under section 1030(a)(5) for "transmission" of harmful code for shipping faulty software. See, e.g. Shaw v. Toshiba Am. Info. Sys., 91 F.Supp.2d 926 (ED Tex. 1999) [mailing floppy diskettes containing faulty microcode]; In re AOL, Inc.Version 5.0 Software Litig., 168 F Supp 2d 1359 (SD Fla. 2001) [AOL's transmission of its Version 5 software which allegedly "changes" the host system's communications configuration and settings so as to interfere with any non-AOL communications and software services actionable under 1030(a)(5)(A)]; Christian v Sony Corp. of Am., 152 F Supp 2d 1184, 1187 (DC Minn. 2001) [shipping personal computers with faulty floppy diskette controllers.] In Christian, though summary judgment was granted for Defendant Sony corporation on damages grounds, the Court believed that the inclusion of a defective FDC constituted a "transmission" within the meaning of section 1030. "[T]he Court was persuaded by the Plaintiffs that Sony's actions could, theoretically, be actionable under the CFAA. For example, Sony's argument that the inclusion of a defective FDC--one which causes corruption of data--in a computer, which was then distributed to individual consumers, does not constitute a 'transmission' within the meaning of the CFAA is not persuasive."

Also, the practice of programming software to shut down under certain circumstances, even to prevent unauthorized use or to enforce contractual obligations, is a potential section 1030 violation. See North Texas Preventative Imaging v. Eisenberg, 1996 U.S. Dist. LEXIS 19990 (C.D. Cal. August 19, 1996); Gomar Manf. Co. v. Novelli, C.A. No. 96-4000 (D.N.J. Jan. 28, 1998).

While these cases are primarily civil, each helps define the activity prohibited by section 1030, "unauthorized access" and "transmission" of harmful code. Increasing punishments for section 1030 offenses potentially increases criminal liability for any of these business practices that also causes $5000 worth of damage. Also, in many of the cases cited above, the lawsuit failed because the threshold damage level was not met. But, the new definition of damage allows harm to be aggregated across acts, victims and time. Under this new definition, practices which were previously the subject of unsuccessful lawsuits, like using cookies or collecting on-line travel data, could be illegal. Internet advertising company DoubleClick, search engine Google.com, Sony, Toshiba and AOL could all be criminally convicted of violation 18 U.S.C. 1030 for common business conduct.

This is a problem that would best be addressed by Congressional amendment of section 1030. However, the Commission must decide whether increased penalties are appropriate. That decision must be informed by the fact that conduct that constitutes an offense under section 1030 is not necessarily serious, malum per se, or even an undesirable business practice.

[1] Many of these cases find no liability under section 1030 based on the plaintiff's failure to allege or prove damages of the proper type or in sufficient amount. The underlying activity, however, is unauthorized access or unlawful transmission within the scope of section 1030.

Additionally, legitimate computer security research and vulnerability reporting is chilled by disproportionate sentencing. For example, port scanning is a common practice among computer security researchers. "A port scan is a method of checking a computer to see what ports are open by trying to establish a connection to each and every port on the target computer. If used by a network administrator on his own network, the scan is a method of determining any possible security weaknesses. If used by an outsider, the scan indicates whether a particular port is used and can be probed for weakness." Moulton v. VC3, 2000 U.S. Dist. LEXIS 19916 (ND Ga. November 7, 2000). Though port scanning is a common tool for security researchers, both in determining vulnerabilities in their own systems and surveying networks for information about deployed programs and security weaknesses, many researchers fear that the activity is arguably illegal under section 1030.

Unfortunately, tales of consultants who are prosecuted criminally or civilly for informing authorities of vulnerabilities are common. A recent cases is that of Stefan Puffer, a computer security analyst who was indicted after demonstrating to the Harris County, Texas District Clerk's office that ITS wireless computer network was vulnerable to unauthorized users. See "County Cuts Off Computer Network", Houston Chronicle, by Steve Brewer, March 21, 2002, available at http://www.chron.com/cs/CDA/story.hts/topstory/1302663#top. See also, "Ethical Hacker Faces War Driving Charges", The Register, by John Leyden, July 26, 2002, available at http://www.chron.com/cs/CDA/story.hts/tech/news/1507766. Many computer security practitioners fearfully view this prosecution as a case of shooting the messenger.

In another recent incident of a computer security practitioner being charged criminally, David McOwen, a PC specialist at Georgia's DeKalb Technical Institute was convicted for participating in a project by the non-profit organization distributed.net that allowed computer users to donate their unused processing power to test the strength of a certain type of encryption. McOwen installed the distributed.net programs on several of the machines he maintained for his employer. Eighteen months later, McOwen was charged under Georgia law with computer trespass. Facing up to 120 years in prison, McOwen decided not to challenge the application of the law to his conduct. Instead, he plead guilty for probation under Georgia's First Offender Act. "Plea Agreement In Distributed Computing Case", SecurityFocus, By Ann Harrison, Jan 18 2002 available at http://www.securityfocus.com/news/311. As a result, computer security professionals fear that distributed computing itself may be illegal. See "Is Distributed Computing A Crime?", SecurityFocus, by Ann Harrison, December 20, 2001 available at http://www.securityfocus.com/news/300. Cases such as McOwen's chill innovation and slow the adoption of valuable new technologies.

People who innocently stumble upon vulnerabilities may also be dissuaded from reporting them. A few years ago, Center for Internet and Society Director Jennifer Granick (also counsel for this submission) received a telephone call from someone who noticed that a co-worker was connecting to the Internet with PC Anywhere file sharing enabled. The caller believed that anyone else could access the co-worker's computer and view files, and successfully tested this theory by doing just that. The caller wanted to notify the co-worker that he was vulnerable and should change his computer configuration, but was afraid to do so, for fear that he would get in trouble for having viewed one of the co-worker's files. The attorney called the co-worker and notified him, keeping the identity of the reporter secret. However, the attorney also

could not give the co-worker the kind of detailed information about why he was vulnerable and how he could fix the problem that the more knowledgeable reporter could. That valuable information was lost in the translation.

Thus, the Commission must act carefully to strike the right balance between deterring crime and chilling business innovation and security research.

II. CURRENT GUIDELINES MAY BE OUT OF LINE WITH THE OFFENDER'S ACTUAL CULPABILITY, AND THE COMMISSION MAY SEE FIT TO AMEND THEM DOWNWARD

The Commission was also directed to consider "the potential and actual loss resulting from the offense, the level of sophistication and planning involved in the offense, 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." Many of these factors are already taken into consideration in the guidelines. A review of the current guidelines suggests that these factors are over-emphasized, and result in a sentence disproportionate to the defendant's culpability.

The current scheme applies the guideline for economic crimes, specifically section 2B1.1, to most computer crimes. Theoretically, treating computer crimes like economic crimes is appropriate since the heartland of the offense is similar. However, Section 1030 crimes are treated *more harshly* than other crimes in several important ways. First, for all practical purposes, the starting offense level for computer crime cases is eight, because almost every computer criminal will receive a two level adjustment for the jurisdictional loss of $5000. Second, computer crimes almost always receive an enhancement for use of special skill in the commission of an offense. (3B1.3, 2B1.1(b)(8)). Third, the calculation of loss in computer crime cases is rife with problems that adjusts the sentence more harshly than in other economic crime cases.

A. The Typical Computer Crime Case Will Be Sentenced At Least As Harshly, If Not More So, Than Other Economic Fraud Cases

Most of the offenses set forth in section 1030 have as an element of the crime that the perpetrator causes $5000 or more in loss. For example, 1030(a)(5)(A) actions are offenses if the defendant caused or would have caused loss aggregated across victims during any one year period, aggregating at least $5000. 18 U.S.C. 1030(a)(5)(B). For violations of section 1030(a)(5)(A)(i), under subsection (c)(2)(B)(iii), if the value of information accessed is over $5000, then the offense is a felony rather than a misdemeanor. Since federal authorities will rarely prosecute misdemeanors, in almost every computer crime case, damages will be at

least $5000. Under Guideline 2B1.1, the Base Offense Level is 6. However, the BOL will be adjusted by at least two levels for loss, giving a minimum offense level of 8 for any prosecuted computer crime. This adjustment is "double counting", since the existence of $5000 of loss makes the offense not only a felony, but also enhances the Base Offense Level. Additionally, it has the effect of sentencing computer crimes more harshly than other economic crime cases.

B. Special Skill

Computer crime offenders disproportionately receive a sentencing enhancement for special skill. Under the pre-2002 guidelines, perpetrators received an adjustment under 3B1.3 for abuse of trust. That section provided that the district court may enhance the defendant's offense level if he "abused a position of public or private trust, or used a special skill, in a manner that significantly facilitated the commission or concealment of the offense." 3B1.3. The phrase "special skill" is defined as "a skill not possessed by members of the general public and usually requiring substantial education, training or licensing. Examples would include pilots, lawyers, doctors, accountants, chemists, and demolition experts." Id. comment. (applic. note 2). The "adjustment applies to persons who abuse their positions of trust or their special skills to facilitate significantly the commission or concealment of a crime. Such persons generally are viewed as more culpable." Id. comment. (backgr'd).

The application of 3B1.3 overstates a defendant's culpability because 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 3B1.3 in computer crime cases. In United States v. Petersen, (9th Cir. 1996) 98 F.3d 502, 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.

If the abuse of trust/special skill adjustment is applied, and the $5000 adjustment applies, then the minimum level at which the most innocuous computer crime offense would be punished is a level 10, not a level 6.

Additionally, there's a special adjustment in 2B1.1 for "sophisticated means" under 2B1.1(b)(8)(B). "'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. If this adjustment is also liberally applied to computer crimes, than 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.

C. The Special Calculation of Loss in Computer Crime Cases Results in Harsher Punishments that That for Comparable Economic Crimes

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. Additionally, the estimation of loss can be manipulated by victims, investigators and prosecutors.

The cost of conducting a damage assessment depends more on the victim's actions than it does on the perpetrator. Assume an intruder compromises two computer systems in identical ways. One victim simply restores the hard drive from backup. The other victim hires $300-an-hour consultants to assess exactly what the intruder did and how he did it. The victim may also ask the consultants to review every other computer system they control, just in case the intruder gained unauthorized access there as well. This is "reasonable". However, in the first instance, the access does not result in loss equal to $5000. The case will probably not be filed, and if it is, the perpetrator will probably not go to jail. In the second instance, the case will be prosecuted and a prison sentence will result. However, the perpetrator's actions and intent are identical.

A similar problem occurs with including any lost revenue due to interruption of service in the loss calculation. Assume one intruder destroys a personal computer, while a second intruder places an unwanted program, like a packet interceptor on an e-commerce computer. The value of the personal computer and the information on it is probably low. The intruder's sentence will be low. In the second instance, the e-commerce server may have to be taken off-line. If the business is small, the loss will be low, but probably higher than the loss the individual has

suffered. If the business is thriving, the loss could be very high. Again, the adjustment the perpetrator receives does not reflect the defendant's relative culpability, but depends on the nature of the victim. Individuals are probably less likely to be able to protect themselves against computer crime, or bounce back from an offense than well-to-do companies. Yet, less real damage on an e-commerce site will probably result in greater prison sentences than malicious destruction of a personal machine. Thus, the definition of loss appears to undermine victim-related adjustments in unwarranted and undesirable ways.

Moreover, loss of 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. Its difficult to estimate whether Yahoo! actually lost any sales or advertising contracts as a result. Yet, some analysts estimated that Yahoo!'s loss would add up to millions of dollars. ZDNet News, February 7, 2000 http://zdnet.com.com/2100-11-518359.html?legacy=zdnn. 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. The attack was perpetrated by a Canadian juvenile who never gained unauthorized access to Yahoo! machines or harmed data on the victim systems. Yet sentencing according to these loss estimates would have resulted in the maximum punishment possible under the law.

Similarly, section 1030(c)(2)(B)(iii) makes theft of data valued at over $5000 a felony offense. Valuing data is extremely difficult. 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, amounting to approximately 80 million dollars. However, the companies were not deprived of the use of that information, nor was it redistributed to competitors, thus reducing its use value. Subsequently, one of the victims started giving the same source code away for free. Additionally, none of the companies reported any economic loss as a result of the intrusions in their SEC filings.

Of course, loss can be difficult to estimate in any economic crime cases. However, this is a serious problem in computer crime cases because loss includes unforeseeable pecuniary harm, losses defined by victim's conduct rather than offense conduct, and more commonly involve the valuation of data and intellectual property. As a result, the loose measure of loss undermines uniformity in sentencing. It also means that loss can be a distorted, or even wholly inaccurate, reflection of the defendant's culpability.

Finally, it means that loss can be structured by victims, law enforcement and prosecutors, to manipulate the number of felonies charged and the sentences for them. In the commentator's experience, victims will be asked for estimates of how much time they spent on the problem, without being informed what type of efforts count towards loss (e.g. damage assessment) and what efforts do not (e.g. improving the security of the system). Victims often do not supply documentation to support their estimates. Rather, they estimate or summarize. The victims do not know that the law imposes limitations on factors that contribute to loss, so they naturally throw in everything.

Law enforcement fails to ensure that loss estimates are reasonable by not providing victims with guidelines to define loss. But the flexible definition of such an important factor leaves sentencing open to manipulation. In one of counsel's cases, the investigating FBI agent sent victims an email instructing that they document as much time spent investigating the problem as possible. For every $5000 they found, the email advised, the government could add another charge.

Similarly, loss has become a huge barga ining chip in plea bargain negotiations. In the beginning of a case, the Department of Justice has early damage estimates based on initial contact with victims during the investigatory stage. Prosecutors will often offer the defendant a plea bargain based on that number. The prosecution tells the defendant that if he does not plead, they will contact victims that did not respond, or re-contact victims to gather additional evidence of damages, thus opening up the possibility of greatly increased loss estimates. Defendants, including those with potentially meritorious defenses, are frightened into entering a plea because the uncertainty of damages means they could do vastly more time in prison once the Department has beaten the bush for numbers from victims.

Loss as currently defined is at risk of completely failing to accurately assess either actual harm, defendant's culpability, or proportionality in sentencing. Also, such vague categories open the sentencing process up to manipulation.

D. The Statute And The Guidelines Do Not Distinguish Between The Culpability Of Offenders Acting With Less Criminal Intent

Relying so heavily on loss as a sentencing factor in computer crime cases misrepresents the defendant's true culpability. This point is further illustrated by the fact that malicious intent to cause harm will be punished less severely than negligent or reckless intent to cause harm if the ultimate loss amount is less. Section 1030(a)(5)(A) sets a maximum of ten years for malicious harm, five years for reckless harm, and one year for unintentional or negligent harm, unless the intrusion was for commercial advantage, in furtherance of another criminal offense or involved the theft of information worth more than $5000. In the first case, the intruder maliciously uses a software program to delete data on the victim computer in violation of 1030(a)(5)(A)(i). The system administrator restores the data from back up in approximately two hours. The maximum sentence ten years. However, even though the defendant acted maliciously, the crime would probably not be charged, because the loss is well below $5000. In the second case, a teenager uses a program he finds on the Internet to get into his school's computer network. While looking around, he unintentionally corrupts the computer database. The school has to purchase new software and hire consultants to try to restore the data. The consultants bill the school for 40 hours of work at $300 an hour. The curious student has amassed $12,000 in damages. The offense would have had a cap of a year in jail. However, the damages exceed $5000, so the maximum is five years. The student would be sentenced at a level 12, or 10 to 16 months. (BOL 6, loss 4, special skill to download and run the program 2).

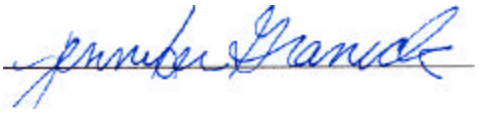
III. CONCLUSION

We encourage the Sentencing Commission to act very carefully with regard to computer crime sentencing. We need to eschew simplistic, expensive, and ineffective tactics like inflexible, harsh sentencing. Those convicted of computer crimes are already punished more harshly compared to similar crimes. Additionally, there are fundamental problems with the way computer crimes sentences are currently determined. These problems should be resolved before the Commission considers new enhancements or penalties. Failure to address these problems, particularly the problem with the special definition of loss including unforeseeable pecuniary harms, USSG $ 2B1.1 Application Note 2(A)(v)(III), results in sentences which are disproportionate to the defendant's culpability and which chill legitimate computer security research, reporting and adoption of new, beneficial technologies. We believe that the Commission should not increase sentences for computer crime offenses. Also, the Commission should consider ways to revise the current scheme to resolve these issues.

Dated: February 19, 2003

Respectfully submitted,

By:



Jennifer Stisa 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

Malcom C. Young, Executive Director
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