



THE GEORGE
WASHINGTON
UNIVERSITY
LAW SCHOOL
WASHINGTON DC

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

January 10, 2003

Re: Request for Public Comment on Responses to Section 225 of the Homeland Security Act of 2002 (the Cyber Security Enhancement Act of 2002), Pub. L. 107-296

Dear Commission:

I 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. In particular, Section 225(b)(2) directs the Commission to :

(A) ensure that the sentencing guidelines and policy statements reflect the serious nature of the offenses [arising under 18 U.S.C. § 1030], the growing incidence of such offenses, and the need for an effective deterrent and appropriate punishment to prevent such offenses;

(B) consider the following factors and the extent to which the guidelines may or may not account for them--

- (i) the potential and actual loss resulting from the offense;
- (ii) the level of sophistication and planning involved in the offense;
- (iii) whether the offense was committed for purposes of commercial advantage or private financial benefit;
- (iv) whether the defendant acted with malicious intent to cause harm in committing the offense;
- (v) the extent to which the offense violated the privacy rights of individuals harmed;
- (vi) whether the offense involved a computer used by the government in furtherance of national defense, national security, or the administration of justice;
- (vii) whether the violation was intended to or had the effect of significantly interfering with or disrupting a critical infrastructure; and
- (viii) whether the violation was intended to or had the effect of creating a threat to public health or safety, or injury to any person

(C) assure reasonable consistency with other relevant directives and with other sentencing guidelines;

(D) account for any additional aggravating or mitigating circumstances that might justify exceptions to the generally applicable sentencing ranges;

(E) make any necessary conforming changes to the sentencing guidelines; and

(F) assure that the guidelines adequately meet the purposes of sentencing as set forth in section 3553(a)(2) of title 18, United States Code.

I am a law professor at the George Washington University Law School, as well as a former Trial Attorney at the Computer Crime and Intellectual Property Section of the United States Department of Justice. I write and teach in the field of computer crime law, including in the area of how the federal sentencing guidelines apply to computer-related crimes. I have also delivered presentations on how the sentencing guidelines apply to Section 1030 offenses at the Federal Sentencing Guidelines seminar held annually in Palm Springs, California, both in 2001 and 2002. The views expressed in this letter are mine alone, and do not reflect the position of either my current or former employers.

In my opinion, the Commission should begin by recognizing the possibility that Congress's directive was based on an erroneous belief: the belief that criminal sentences for computer criminals under the current versions of the Federal Sentencing Guidelines are lower than sentences for other criminals who commit analogous crimes off-line. This is not true. In fact, the United States Sentencing Guidelines already treat computer criminals as harshly *if not more harshly* than those who commit equivalent crimes off-line. This does not mean that Congress was wrong in its apparent belief that the computer crime laws need to be amended. Those laws do need attention. However, sentencing issues under 18 U.S.C. § 1030 arise only *after* the government has successfully investigated a case and obtained a conviction under the statute, which happens in only about 70 or 80 cases each year. The sentences that are obtained in these small number of cases are not a major problem in the field of computer crime law. The primary difficulties with the current laws arise primarily in the investigative stage, not among the few cases that actually lead to a conviction. As a result, the Commission should proceed cautiously, and should not take the vague directive in the recent law as an invitation to rewrite from scratch the law of sentencing for computer criminals.

It is important for the Commissioners to understand why the current sentencing law treats computer criminals just as seriously (if not more seriously) than others convicted of federal crimes. To begin with, calculations of sentences under the current guidelines under the most commonly used portions of 18 U.S.C. § 1030 -- sub-sections (a)(2), (a)(4), and (a)(5) -- apply the same "economic crimes" packages under 2B1.1 of the Federal Sentencing Guidelines that apply to other economic crimes. This means that the basic calculations of computer crime offenses match those of other crimes. In fact, Section 1030 crimes are treated *more harshly* than other crimes in one important respect: while the calculation of economic losses are generally limited to "reasonably foreseeable pecuniary harm," the current guidelines have a special rule for Section 1030 offenses that involve "unlawfully accessing, or exceeding authorized access" to a computer. (It is unclear whether this special rule was intended to apply to all Section 1030 offenses, or just the subset of cases involving exceeding access to a protected computer.) In such cases, even nonforeseeable pecuniary harms can be included, including "*any* lost revenue due to interruption of service." USSG § 2B1.1 Application Note 2(A)(v)(III) (emphasis added). The effect of this special rule is to treat computer crimes more harshly than other crimes. For example, a computer hacker whose activity inadvertently shuts down an e-commerce site, causing the site a loss of \$5,000,000, could be treated the same as a con man who intentionally bilks his victims out of \$5,000,000. In the case of a computer hacker, the unforeseeable loss to the victim that did not benefit the hacker would be used to increase his sentence, while in the

case of the con man, only foreseeable losses (and mostly those that directly benefit the defendant) would count.

The current guidelines also account for several nonpecuniary dynamics of computer crimes that arguably warrant special treatment. Most if not all of the factors that Congress points to in its directive are already considered by the current guidelines. For example, Section 3B1.3 of the guidelines already provide for a two-level upward adjustment for use of a "special skill," which has been applied to computer hacking cases. *See, e.g., United States v. Petersen*, 98 F.3d 502 (9th Cir. 1996). The current guidelines also allow for an upward departure for offenses that "result[] in a substantial invasion of privacy interest", USSG § 2B1.1 Application Note 15(A)(ii), which may apply in computer crime offenses that involve important privacy concerns. Finally, the relevance of committing an offense for commercial advantage or private financial gain to the seriousness of the offense is already drawn in Section 1030 itself. *See, e.g., 18 U.S.C. § 1030(c)(2)(B)(i)*. Because of these provisions, current law *already* contain means by which the sentence of computer criminals can be raised in special cases if appropriate.

Despite this, the Commission may feel that faithfully implementing Congress's directive may require the Commission to increase the penalties for violations of Section 1030. One obvious precedent for such an approach would be a provision such as USSG § 2G2.4(b)(3), effective on November 1, 1996, which triggers a two-level enhancement in offenses involving possession of child pornography when the possession "resulted from the defendant's use of a computer." As the Ninth Circuit explained in *United States v. Fellows*, 157 F.3d 1197, 1202 (9th Cir. 1998), this section "provides an extra deterrent to those inclined to pursue illicit pictures in the anonymity of the computer world." The Commission could adopt this approach for Section 1030 offenses, as well. The reasoning would go something like this: computer misuse crimes such as hacking and denial-of-service attacks are easy to commit, and the anonymity of the Internet makes such offenses difficult to trace, such that an extra punishment for computer misuse may be helpful to deter the misconduct. In effect, the law may want to counteract the effect of the technology: as the technology lowers the barriers to committing such offenses, the sentencing enhancement may raise the cost that the criminal law imposes to compensate for the difference.

The difficulty with such a sentencing enhancement is that to the extent such a rationale is convincing, it should apply to all computer crimes, not just the subset of computer crimes charged under 18 U.S.C. § 1030. The actual and perceived anonymity of the Internet tends to lower the perceived cost of several types of crimes. Often those who commit crimes online would be disinclined to commit an equivalent crime offline; they see the Internet as somehow less real, less connected to actual human beings and actual harms. From the standpoint of the traditional theories of punishment underpinning criminal law reflected in 18 U.S.C. § 3553(a)(2), this presents a mixed bag. On one hand, a utilitarian approach might suggest that greater punishment is warranted to deter the harmful conduct. *See 18 U.S.C. § 3552(a)(2)(B),(C)*. On the other hand, from the standpoint of retributive theory, *see 18 U.S.C. § 3552(a)(2)(A)*, widespread public perceptions that offenses involving the Internet are somehow less real may make such offenses less morally culpable. If those who commit crimes online do not confront the societal implications of their misconduct as directly as those who commit offline crimes do,

the commission of the online crime may on average reflect less moral depravity than the commission of otherwise equivalent offline crime, suggesting that *lesser* punishments may be more appropriate for the online misconduct.

My own view is that these two competing arguments roughly cancel out, such that it generally makes sense to apply the same punishments to analogous misconduct that occurs off-line and on-line. However, if the Commission finds the deterrence argument for online misconduct persuasive, it is unclear why the Commission would want to limit a possible enhancement to Section 1030 offenses. Not only would such a strategy create a new plea bargaining tool for the Department of Justice (prosecutors could accept pleas under the wire fraud statute instead of the computer fraud provision of section 1030, for example), but it would artificially treat Section 1030 offenses differently than other computer crimes for no convincing reason. Perhaps the most coherent strategy would be to take the principle of § 2G2.4(b)(3) and apply it to convictions arising from *any* criminal act facilitated or encouraged by the perceived or actual anonymity of the Internet.

To summarize, current law already appears to track the concerns that motivated Congress to pass Section 225(b) of the Homeland Security Act. The Commission should therefore not respond to Congress's directive with drastic changes to the sentencing provisions that apply to convictions under Section 1030. To the extent that changes are warranted, they should generally work towards eliminating differences between how the guidelines treat 1030 and other offenses, not creating new differences. However, if the Commission believes that faithfully implementing Congress's directive requires it to enact some kind of sentencing enhancement for computer crimes, the Commission should consider a broad enhancement reflecting how the Internet changes the perceived risks and harms of criminal conduct, rather than one artificially tailored to Section 1030 offenses or a subset of such offenses.

Sincerely,



Orin S. Kerr
Associate Professor
George Washington University
Law School
2000 H Street, NW
Washington DC 20052
(202) 994-4775
okerr@law.gwu.edu