

## **PROPOSED ISSUE FOR COMMENT #1: IMPLEMENTATION OF THE WIRELESS TELEPHONE PROTECTION ACT**

**Synopsis:** The Wireless Telephone Protection Act, Pub. L. 105–418 (the "Act"), provides a general directive to the Commission to review and amend, if appropriate, the guidelines and policy statements to provide an appropriate penalty for offenses involving the cloning of wireless telephones, including attempts and conspiracies.<sup>1</sup> (See attached for a copy of the directive.)

The Act also amends 18 U.S.C. § 1029 (Fraud and related activity in connection with access devices) to eliminate the intent to defraud element with respect to persons who knowingly use, produce, traffic in, have custody or control of, or possess hardware (a "copycat box") or software which has been configured for altering or modifying a telecommunications instrument.<sup>2</sup> This amendment effectively creates a presumed intent. Accordingly, the government only has to prove that the defendant knowingly used or possessed the hardware or software with the knowledge that it had been configured for modifying a cellular phone so that the phone could be used to obtain unauthorized access to telecommunications services. The legislative history indicates that this portion of the Act addresses law enforcement's concern with the difficulty of proving the current provisions's "intent to defraud" element. Often law enforcement find the cloning equipment while arresting an individual for another crime. Although there is no legitimate reason for possessing the equipment unless the person works in the telecommunications industry, law enforcement often cannot prove that the equipment was possessed with the intent to defraud.

Cloning occurs when a cellular phone's electronic serial number ("ESN") and mobile identification number ("MIN"), both of which are transmitted to the telecommunications company

---

<sup>1</sup>In carrying out this directive, the Commission shall consider, among other things:

- the range of conduct covered by the offense;
- the existing sentences for such offenses;
- the extent to which loss is an adequate measurement for establishing penalties for such offenses;
- the extent to which other guideline adjustments and departures permit courts to sentence at or near the maximum penalty for the most serious offenders;
- the extent to which current guideline penalties are constrained by statutory maximums;
- the extent to which the guidelines for such offenses achieve the purposes of sentencing (18 U.S.C. § 3553(a)(2));
- the relationship of guidelines for "cellular phone fraud" and other offenses of comparable seriousness;
- any other factor the Commission considers appropriate.

<sup>2</sup>This offense was formerly covered by subsection (a)(8); the legislation creates a new subsection (a)(9) for the offense.

when the phone is in use, are obtained from the airwaves through the use of a scanning receiver. These numbers can then be embedded into another cellular phone (the "clone") with either special hardware (known as a "copycat box") or a personal computer equipped with special software. A clone can be made in less than one minute simply by attaching a cellular phone to the copycat box through the phone's "port" and downloading the ESN / MIN combination. The legitimate cellular phone user is then charged for any calls made with the cloned phone. Congress is concerned that such offenses are not punished as severely as they should be in light of the magnitude of loss resulting from this crime<sup>3</sup> and the fact that this crime is often used to facilitate more serious crimes, in particular, drug offenses.

The following "Issue for Comment" is proposed to preserve the Commission's options for future consideration:

**Proposed Issue for Comment:**

*The Wireless Telephone Protection Act, Pub.L. 105-418 (the "Act"), provides a general directive to the Commission to review and amend, if appropriate, the sentencing guidelines and policy statements to provide an appropriate penalty for offenses involving the cloning of wireless telephones, including attempts and conspiracies. The Commission invites comment on whether and how it should amend the guidelines for offenses involving the cloning of wireless telephones, including offenses involving an attempt or conspiracy to clone a wireless telephone. See 18 U.S.C. § 1029(e)(9) (as amended by the Act).*

*Specifically, should the Commission amend §2F1.1 (Fraud), the guideline to which such offenses are referenced, to provide a tailored enhancement (specific offense characteristic) if the offense, including any relevant conduct, involved the use of hardware (a "copycat box") or software which has been configured for altering or modifying a wireless telephone? If so, what should be the magnitude of such an enhancement? Should the Commission provide a specific offense characteristic in §2F1.1, or a cross reference to other offense guidelines, if the cloning offense facilitated, or was in connection with, another offense? If such a specific offense characteristic or a cross reference is warranted, by how many levels should the sentence for such offenders be increased?*

[Note: A vote on this is a vote on whether to publish the issue in the Federal Register.]

---

<sup>3</sup>The wireless telephone industry reports losing hundreds of millions of dollars in revenue each year to calls made from cloned or stolen cellular telephones. For example, the industry reports losing \$710 million in 1996 (the last year for which data is available) to such activity. However, as of the time of this memorandum, the Sentencing Commission does not know how much dollar loss is involved in the average case.

