elw

# UNITED STATES SENTENCING COMMISSION

## PUBLIC HEARING

Thursday, March 23, 2000

Judicial Conference Center
1 Columbus Circle, N.E.
Washington, D.C.

The public hearing convened, pursuant to notice, at 9:30 a.m., The Honorable Diana E. Murphy, Judge, United States Court of Appeals (8th Circuit), Chair, presiding.

MILLER REPORTING CO., INC.
507 C STREET, N.E.
WASHINGTON, D.C. 20002
(202) 546-6666

COMMISSIONER SESSIONS: So Congress was in fact directing the legislation toward the copyright industry, but your sources have said that it is--

MR. QUAM: My sources said that this directive that calls for an enhancement of the sentencing is meant to apply to all intellectual property, not just copyrights.

CHAIR MURPHY: You know, I have got an unpleasant task, because unless I keep us moving, we are not going to be able to hear all the panels.

COMMISSIONER SESSIONS: You want to know who the sources are?

COMMISSIONER KENDALL: No, I just want to know if your sources had talked to their sources.

MR. KRUGER: They may be on different sides of the aisle.

CHAIR MURPHY: Mr. Kruger, Mr. Quam, we really appreciate your being here on behalf of your groups, and you can see that we are engaged, and we appreciate your help.

MR. KRUGER: Thank you.

MR. QUAM: Thank you.

CHAIR MURPHY: The next panel is on cellular telephone

cloning and identity theft, and we have Roseanna DeMaria on telephone cloning. She is the Senior Vice President, Business Security, AT&T Wireless Services. We have got Mary Riley on cloning also, Assistant Special Agent in Charge of the United States Secret Service. And on identity theft we have Edward Kitlas, who is Assistant Special Agent in Charge of the Secret Service. And so we will start with Ms. DeMaria.

MS. DeMARIA: Judge Murphy, members of the Commission, thank you for the opportunity, for letting us be heard this morning.

I come to you this morning to ask you to reconsider identity theft, not as a crime as an end in itself, but as the modus operandi of the criminal entrepreneur of the millennium. He or she will use that operandi to erode our constitutional values of property and privacy. It needs to be looked at for a uniform approach in sentencing that sends a message of deterrence and zero tolerance.

To enhance that look at it, I bring with me the lessons learned in the cloning war. I have a number of the scars

with me and they will never leave me. And I bring with me the future, which is now, technological convergence.

The lessons learned in the cloning wars I learned in two places. One was in the Office of the Special Narcotics Prosecutor with The Honorable Sterling Johnson, and I learned it at the hands of the Cali cartel, the most accomplished equivalent of the dot com in the criminal world. They used cloned phones because of the anonymity those phones provided them to ply their trade and to evade the law enforcement. They weren't interested in stealing phone service. They didn't care about other people's identity. They wanted to run away from law enforcement and ply their trade.

When I joined AT&T Wireless, I learned that the industry as well as the legislatures looked at cloning as a theft of services crime; that these folks were stealing phone services. Phone theft had been around forever, and industry figures were rampant. They were in the news. We all read about it. At its height, it accounted for 3.8 percent of the revenue of the wireless phone industry.

Everyone thought it was about stealing service. To be sure, there will always be folks out there stealing phone service. In the beginning, when a service industry opened, whether it was restaurants or credit cards or banks, there was theft of services. That is not what cloning was about and it is not what identity theft is about.

You know, when these cases started to be prosecuted in the Federal Government, thanks to the innovative approach of the Secret Service and DEA, the District Courts were split on whether these cloned phones were at risk devices. Well, let me tell you, from the State perspective, try to argue to a State judge that that cellular phone is a forged instrument. It is not a pretty argument. It doesn't look like a duck, it doesn't quack like a duck. It is a cellular phone, and what was being stolen was the electronic serial number and the mobile ID number. You can't touch it, you can't smell it, you can't feel it. It is not a tangible piece of property.

Well, what it was about was anonymity. We were measuring it wrong. We were looking at it as industry losses. What that

industry loss number tells you is the scope of criminal demand for anonymity, and I suggest to you that the large majority of those criminal users were using it as an approach to ply their trade.

What is the true loss? Well, I learned that where we learn most of our things in the wireless industry, from our customers. We held focus groups, because AT&T Wireless wanted to put out billboards that said to the criminal, "The wireless phone has gotten very sophisticated now. We can track the folks who steal it," and we were concerned that that would scare our customers. When we held focus groups, our customers were outraged that there was an ESN/MIN that belonged to them, that even though they didn't pay for those losses, was being stolen.

I would analogize it to this. Imagine going on vacation, and while you were gone, a large criminal entrepreneur like the Cali cartel came in. They held business. They didn't break through your door. There was no disruption or damage to your property. They conducted business, and they left, secured your premises, and you come back home. You suffered

no monetary damage, but you were invaded. You were the last to know. You didn't even know it happened.

In fact, our customers are always the last to know. When we find it, we take it off of the bill so it doesn't disrupt their services. Their property rights are being invaded. Our notions of constitutional property and privacy are being invaded.

Loss numbers? If that one phone call on a cloned phone is to order a murder or a delivery of drugs, or to warn a confederate that there is a law enforcement officer coming up behind a fellow criminal, what is the loss of that phone call? I would suggest to you that that one phone call has a tremendous loss, and it has nothing to do with the cost of the lost opportunity on that service.

To suggest that loss is relevant in this context is the equivalent of using a tape measure to measure a (inaudible). It is not worthy. The lesson that I take from that is, (inaudible) ESN/MIN numbers, should we consider losses--

CHAIR MURPHY: I think that, you know, we have been studying the submissions and the concerns, and Congress has indicated

concerns to us. We are aware of those, and what we are dealing with now is, well, what is the best way to address this? And are you going to speak to that? Because here again we have limited time, we have got three people, and while it is fine to address the overall concern and you do it in a very striking way, what should we do specifically here, you know?

MS. DeMARIA: I think you have a unique opportunity, Judge Murphy, to look at identity theft for a uniform sentencing approach that is not technology specific. What we are talking about in the Wireless Telephone Protection Act is a technology-specific approach.

That becomes meaningless in the world of the future which involves technological convergence, with the explosion of the internet, with e-commerce, with the coming of the virtual customer, we will morph to a world in telecommunications and broad band where we will never see our customer. It will be anytime, anywhere, voice and data, mobile and fixed. You won't be able to touch it.

Identity theft then expands like a toxic gas to fill the

container of that technological opportunity. I think if identity theft were studied in that context, you would be able to put together a grid of factors that could be calculated in terms of its true impact, not only to the big risks that are currently existing in technological-specific crimes like you have here but in the context of the risk to the future. If customers do not have confidence in the system, they won't empower it, and then the world of on-line banking, on-line trading, e-commerce, the world of technological convergence and all the promise and value it brings to the American consumer--

COMMISSIONER JOHNSON: Let me say first, nice to see you again. I have fond memories of our work together. But these options we have to consider, are you saying that you favor none of these options?

MS. DeMARIA: No, Your Honor. We endorse Option 3, and the reason we endorse Option 3 is, it recognizes the nexus between the Identity Theft Act and the Wireless Telephone Protection Act, which I believe was its intent. It gives a broad definition of access divides, and it increases law.

What I am suggesting to you, it is not enough. The criminal personality moves at the speed of internet crime. I think if we go with the limited approach here, we are not sending the necessary message. I think the changing criminal frontier demands a re-look at this and a uniform sentencing approach with gradations across all crimes. We need to address this. I think our constitutional values mandate it, and I think the American consumer--

COMMISSIONER JOHNSON: So from the industry's point of view, Option 3 is a first step?

MS. DeMARIA: Option 3, yes.

COMMISSIONER KENDALL: One other question, and you can address it. I am a little surprised to hear an AT&T Wireless person say that the greater harm is the criminal using a cloned phone, rather than the loss that occurs from the usage of that phone.

MS. DeMARIA: That's fair.

COMMISSIONER KENDALL: Is that fair? One thing we talked about, although staff didn't address specific language for it but it has been discussed, is a general enhancement for

use of a cloned phone in any criminal activity, and that would be maybe an adjustment in Chapter 3, just like to get points for other specific conduct across a broad spectrum of offenses. What would be your comment with regard to that? I assume you are supportive of that?

MS. DeMARIA: Enthusiastically. We have supported that in a number of State legislative initiatives. But again, the proper math is, we are talking about the phone. The phone will morph in the very near future into your connection to the internet, your connection to the bank. I think you have to move away from the clone-specific approach and think about it in the context of technological conversion.

COMMISSIONER KENDALL: To what?

MS. DeMARIA: Just briefly, the phone that gives you the internet, that also reads bar codes in supermarkets so that you can indicate what you want to the cashier. The broad definition of access device that is endorsed by Option 3, I would suggest that you stop talking about ESN/MIN. I think we have defined an ESN/MIN as an access device. Broaden it to meet the speed of technology.

CHAIR MURPHY: I would like to move on, and we may be able to get back with some questions with you, Ms. DeMaria. We really appreciate your presence here, but I would like to get to the Secret Service.

COMMISSIONER JOHNSON: I just want to say one thing.

CHAIR MURPHY: All right, Judge Johnson.

COMMISSIONER JOHNSON: Ms. DeMaria is one of the best prosecutors I ever had. You can order a transcript.

CHAIR MURPHY: Ms. Riley, you are next.

MS. RILEY: Good morning. Thank you. I appreciate the opportunity to address this phase of the process to make amendments to 1029. As an agent involved in these offenses for the last 13 years, I have been very close to this issue throughout, and now serving at our headquarters, have the opportunity to review these cases as they come in throughout our 165 field offices.

One of the top concerns we had in working on the drafting that occurred as a joint initiative between industry and law enforcement in this case was the issue of the source of the types of fraud that were occurring, and that is plainly